ESET NOD32 ANTIVIRUS 9

Guida dell'utente

(per la versione 9.0 e le versioni successive del prodotto)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / XP

Fare clic qui per scaricare la versione più recente di questo documento

ENJOY SAFER TECHNOLOGY™

ESET NOD32 ANTIVIRUS

Copyright ©2015 di ESET, spol. s r. o.
ESET NOD32 Antivirus è stato sviluppato da ESET, spol. s r. o.
Per ulteriori informazioni, visitare il sito Web www.eset.it.
Tutti i diritti riservati. Sono vietate la riproduzione, l'archiviazione in sistemi di registrazione o la trasmissione in qualsiasi forma o con qualsiasi mezzo, elettronico, meccanico, tramite fotocopia, registrazione, scansione o altro della presente documentazione in assenza di autorizzazione scritta dell'autore.
ESET, spol. s r. o. si riserva il diritto di modificare qualsiasi parte dell'applicazione software descritta senza alcun preavviso.

Assistenza clienti nel mondo: www.eset.it/supporto

REV. 10/6/2015

Contenuti

1. ESET NOD32 Antivirus.....5
1.1 Novità della versione 9.....6
1.2 Requisiti di sistema.....6
1.3 Prevenzione.....6
2. Installazione.....8
2.1 Live installer.....8
2.2 Installazione off-line.....9
2.2.1 Impostazioni avanzate.....10
2.3 Problemi di installazione comuni.....11
2.4 Attivazione prodotto.....11
2.5 Inserimento della chiave di licenza.....11
2.6 Aggiornamento a una versione più recente.....12
2.7 Primo controllo dopo l'installazione.....12
3. Guida introduttiva.....13
3.1 La finestra principale del programma.....13
3.2 Aggiornamenti.....15
4. Utilizzo di ESET NOD32 Antivirus.....17
4.1 Protezione del computer.....18
4.1.1 Antivirus.....19
4.1.1.1 Protezione file system in tempo reale.....20
4.1.1.1.1 Parametri ThreatSense aggiuntivi.....21
4.1.1.1.2 Livelli di pulizia.....21
4.1.1.1.3 Quando modificare la configurazione della protezione in tempo reale.....22
4.1.1.1.4 Controllo della protezione in tempo reale.....22
4.1.1.1.5 Cosa fare se la protezione in tempo reale non funziona.....22
4.1.1.2 Controllo del computer.....23
4.1.1.2.1 Launcher controllo personalizzato.....24
4.1.1.2.2 Avanzamento controllo.....25
4.1.1.2.3 Profili di scansione.....26
4.1.1.3 Controllo all'avvio.....26
4.1.1.3.1 Controllo automatico file di avvio.....26
4.1.1.4 Controllo stato inattivo.....27
4.1.1.5 Esclusioni.....27
4.1.1.6 Parametri di ThreatSense.....28
4.1.1.6.1 Pulizia.....33
4.1.1.6.2 Estensioni file esclusi dal controllo.....34
4.1.1.7 Rilevamento di un'infiltrazione.....34
4.1.1.8 Protezione documenti.....36
4.1.2 Supporti rimovibili.....36
4.1.3 Controllo dispositivi.....37
4.1.3.1 Editor regole controllo dispositivi.....38
4.1.3.2 Aggiunta di regole per il controllo dispositivi.....39
4.1.4 Sistema anti-intrusione basato su host (HIPS).....40
4.1.4.1 Configurazione avanzata.....42
4.1.4.2 Finestra interattiva HIPS.....43
4.1.5 Modalità giocatore.....43
4.2 Protezione Internet.....44
4.2.1 Protezione accesso Web.....45
4.2.1.1 Di base.....46
4.2.1.2 Protocolli Web.....46
4.2.1.3 Gestione indirizzo URL.....46
4.2.2 Protezione client di posta.....47
4.2.2.1 Client di posta.....47
4.2.2.2 Protocolli e-mail.....48
4.2.2.3 Avvisi e notifiche.....49
4.2.2.4 Integrazione con client e-mail.....50
4.2.2.4.1 Configurazione della protezione client di posta.....50
4.2.2.5 Filtro POP3, POP3S.....50
4.2.3 Filtraggio protocolli.....51
4.2.3.1 Web e client di posta.....51
4.2.3.2 Applicazioni escluse.....52
4.2.3.3 Indirizzi IP esclusi.....53
4.2.3.3.1 Aggiungi indirizzo IPv4.....53
4.2.3.3.2 Aggiungi indirizzo IPv6.....53
4.2.3.4 SSL/TLS.....54
4.2.3.4.1 Certificati.....55
4.2.3.4.2 Elenco di certificati noti.....55
4.2.3.4.3 Elenco di applicazioni filtrate tramite SSL.....56
4.2.4 Protezione Anti-Phishing.....56
4.3 Aggiornamento del programma.....57
4.3.1 Impostazioni di aggiornamento.....60
4.3.1.1 Aggiorna profili.....62
4.3.1.2 Impostazione aggiornamento avanzata.....62
4.3.1.2.1 Modalità di aggiornamento.....62
4.3.1.2.2 Proxy HTTP.....62
4.3.1.2.3 Connetti a LAN come.....63
4.3.2 Rollback aggiornamento.....64
4.3.3 Come creare attività di aggiornamento.....65
4.4 Strumenti.....66
4.4.1 Strumenti in ESET NOD32 Antivirus.....66
4.4.1.1 File di rapporto.....67
4.4.1.1.1 File di rapporto.....68
4.4.1.1.2 Microsoft NAP.....69
4.4.1.2 Processi in esecuzione.....70
4.4.1.3 Statistiche di protezione.....71
4.4.1.4 Attività di verifica.....72
4.4.1.5 ESET SysInspector.....73
4.4.1.6 Pianificazione attività.....73
4.4.1.7 ESET SysRescue.....75
4.4.1.8 ESET LiveGrid®.....75
4.4.1.8.1 File sospetti.....76
4.4.1.9 Quarantena.....77
4.4.1.10 Server proxy.....78
4.4.1.11 Notifiche e-mail.....79
4.4.1.11.1 Formato dei messaggi.....80
4.4.1.12 Seleziona campione per analisi.....81
4.4.1.13 Aggiornamento Microsoft Windows®.....81

4.5 Interfaccia utente....82
4.5.1 Elementi dell'interfaccia utente....82
4.5.2 Avvisi e notifiche....84
4.5.2.1 Configurazione avanzata....85
4.5.3 Finestre di notifica nascoste....85
4.5.4 Configurazione dell'accesso....86
4.5.5 Menu del programma....87
4.5.6 Menu contestuale....88

5. Utente avanzato....89

5.1 Gestione profili....89
5.2 Tasti di scelta rapida....89
5.3 Diagnostica....90
5.4 Importa ed esporta impostazioni....90
5.5 Rilevamento stato inattivo....91
5.6 ESET SysInspector....91
5.6.1 Introduzione a ESET SysInspector....91
5.6.1.1 Avvio di ESET SysInspector....91
5.6.2 Interfaccia utente e utilizzo dell'applicazione....92
5.6.2.1 Comandi del programma....92
5.6.2.2 Navigare in ESET SysInspector....94
5.6.2.2.1 Tasti di scelta rapida....95
5.6.2.3 Confronta....96
5.6.3 Parametri della riga di comando....97
5.6.4 Script di servizio....98
5.6.4.1 Generazione dello script di servizio....98
5.6.4.2 Struttura dello script di servizio....98
5.6.4.3 Esecuzione degli script di servizio....101
5.6.5 Domande frequenti....102
5.6.6 ESET SysInspector come componente di ESET NOD32 Antivirus....103
5.7 Riga di comando....103

6. Glossario....106

6.1 Tipi di infiltrazioni....106
6.1.1 Virus....106
6.1.2 Worm....106
6.1.3 Trojan horse....106
6.1.4 Rootkit....107
6.1.5 Adware....107
6.1.6 Spyware....107
6.1.7 Programmi di compressione....108
6.1.8 Applicazioni potenzialmente pericolose....108
6.1.9 Applicazioni potenzialmente indesiderate....108
6.2 Tecnologia ESET....111
6.2.1 Exploit Blocker....111
6.2.2 Scanner memoria avanzato....112
6.2.3 ThreatSense....112
6.2.4 Java Exploit Blocker....112
6.3 E-mail....113
6.3.1 Pubblicità....113
6.3.2 Hoax: truffe e bufale....113
6.3.3 Phishing....114
6.3.4 Riconoscimento messaggi spamming....114

7. Domande comuni....115

7.1 Come aggiornare ESET NOD32 Antivirus....115
7.2 Come rimuovere un virus dal PC....115
7.3 Come creare una nuova attività nella Pianificazione attività....116
7.4 Come pianificare un controllo del computer settimanale....116

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus rappresenta un nuovo approccio alla protezione effettivamente integrata del computer. La versione più recente del motore di controllo ThreatSense® sfrutta la velocità e la precisione per proteggere il computer. Il risultato è un sistema intelligente che rileva continuamente attacchi e software dannoso che potrebbero minacciare il computer.

ESET NOD32 Antivirus è una soluzione di protezione completa che associa massime prestazioni a un impatto minimo sul sistema. Le tecnologie avanzate utilizzano l'intelligenza artificiale per prevenire l'infiltrazione da parte di virus, spyware, trojan horse, worm, adware, rootkit e altre minacce senza ripercussioni sulle prestazioni del sistema o interruzioni del computer.

Funzioni e vantaggi

Interfaccia utente rinnovata	L'interfaccia utente nella versione 9 è stata notevolmente migliorata e semplificata a seguito dei risultati dei test di usabilità. Tutti i termini e le notifiche dell'interfaccia grafica utente sono stati accuratamente rivisti e l'interfaccia offre ora il supporto per le lingue scritte da destra a sinistra quali l'ebraico e l'arabo. **La Guida online** è ora integrata in ESET NOD32 Antivirus e offre contenuti di supporto aggiornati a livello dinamico.
Antivirus e antispyware	Rileva e pulisce in modo proattivo virus, worm, trojan e rootkit noti e sconosciuti. L'**Euristica avanzata** rileva persino malware mai rilevati in precedenza, proteggendo l'utente da minacce sconosciute e neutralizzandole prima che possano arrecare danni al sistema. La **Protezione accesso Web** e **Anti-Phishing** monitora la comunicazione tra i browser Web e i server remoti (compreso il protocollo SSL). La **Protezione client di posta** garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3(S) e IMAP(S).
Aggiornamenti periodici	L'aggiornamento periodico del database delle firme antivirali e dei moduli del programma rappresenta la soluzione migliore per ottenere il livello massimo di protezione del computer.
ESET LiveGrid® (Reputazione basata sul cloud)	È possibile controllare la reputazione dei processi e dei file in esecuzione direttamente da ESET NOD32 Antivirus.
Controllo dispositivi	Controlla automaticamente tutte le memorie USB, le schede di memoria e i CD/DVD. Blocca i supporti rimovibili in base al tipo di supporto, al produttore, alle dimensioni e ad altri attributi.
Funzionalità HIPS	È possibile personalizzare il comportamento del sistema in maggiori dettagli, specificando le regole per il registro di sistema, i processi e i programmi attivi e ottimizzando il livello di protezione.
Modalità giocatore	Rimanda tutte le finestre popup, gli aggiornamenti o altre attività di sistema intensive allo scopo di preservare le risorse di sistema per le attività di gioco e altre attività a schermo intero.

Affinché le funzioni di ESET NOD32 Antivirus siano attive, è necessario attivare una licenza. Si consiglia di rinnovare la licenza di ESET NOD32 Antivirus alcune settimane prima della scadenza.

1.1 Novità della versione 9

La versione 9 di ESET NOD32 Antivirus presenta i seguenti miglioramenti:

- **Interfaccia grafica rinnovata**: l'interfaccia grafica di ESET NOD32 Antivirus è stata completamente rinnovata allo scopo di garantire una visibilità ottimizzata e un'esperienza utente più intuitiva. L'interfaccia offre ora il supporto per le lingue scritte da destra a sinistra quali l'ebraico e l'arabo. **La Guida online** è ora integrata in ESET NOD32 Antivirus e offre contenuti di supporto aggiornati a livello dinamico.
- **Installazione più rapida e affidabile** - Comprende l'avvio di un primo controllo automatico 20 minuti dopo l'installazione o il riavvio.

Per ulteriori informazioni sulle nuove funzionalità di ESET NOD32 Antivirus, consultare il seguente articolo della Knowledge base ESET:
Novità in ESET Smart Security 9 ed ESET NOD32 Antivirus 9

1.2 Requisiti di sistema

Per il corretto funzionamento di ESET NOD32 Antivirus, il sistema deve soddisfare i seguenti requisiti hardware e software:

Processori supportati: Intel® o AMD x86-x64
Sistemi operativi: Microsoft® Windows® 10/8.1/8/7/Vista/XP SP3 a 32 bit/XP SP2 a 64 bit/Home Server 2003 SP2 a 32 bit/Home Server 2011 a 64 bit

1.3 Prevenzione

Quando si utilizza il computer, e in particolare quando si naviga in Internet, occorre tenere presente che nessun sistema antivirus al mondo può eliminare completamente il rischio di infiltrazioni e attacchi. Per garantire la massima protezione e comodità, è essenziale utilizzare correttamente la soluzione antivirus e attenersi ad alcune regole utili:

Eseguire regolarmente l'aggiornamento

In base alle statistiche ottenute da ThreatSense, ogni giorno vengono create migliaia di infiltrazioni nuove e uniche per aggirare le misure di sicurezza esistenti e generare profitti per i rispettivi autori, a spese e discapito di altri utenti. Gli specialisti del laboratorio di ricerca ESET analizzano queste minacce su base giornaliera, preparando e rilasciando gli aggiornamenti per migliorare costantemente il livello di protezione degli utenti. Per garantire l'efficacia massima di questi aggiornamenti, è importante che questi vengano configurati correttamente sul sistema. Per ulteriori informazioni su come configurare gli aggiornamenti, consultare il capitolo Impostazione dell'aggiornamento.

Scaricare le patch di protezione

Gli autori di software dannoso sfruttano spesso le varie vulnerabilità dei sistemi per aumentare l'efficacia della diffusione di codice dannoso. In considerazione di ciò, le società di software esaminano attentamente eventuali vulnerabilità nelle applicazioni create e rilasciano regolarmente gli aggiornamenti di protezione allo scopo di eliminare le potenziali minacce. È importante scaricare questi aggiornamenti della protezione non appena vengono rilasciati. Microsoft Windows e i Web browser quali Internet Explorer sono due esempi di programmi per cui gli aggiornamenti di protezione vengono rilasciati periodicamente.

Eseguire il backup dei dati importanti

Di norma, gli autori di malware non sono interessati alle esigenze degli utenti e l'attività dei programmi dannosi comporta spesso un malfunzionamento generale del sistema operativo e la perdita di dati importanti. È importante eseguire un backup periodico dei dati importanti e sensibili su un supporto esterno, ad esempio un DVD o un'unità hard disk esterna. Ciò consente di recuperare i dati in modo semplice e veloce in caso di errore del sistema.

Eseguire regolarmente la scansione antivirus

Il rilevamento di virus, worm, trojan e rootkit più noti e sconosciuti è gestito dal modulo della protezione file system in tempo reale. Ciò significa che ad ogni accesso ad un file o apertura dello stesso da parte dell'utente, questo viene controllato per la ricerca di attività malware. Si consiglia di eseguire un Controllo del computer completo almeno una volta al mese, in quanto le firme dei malware cambiano continuamente e il database delle firme antivirali si aggiorna con frequenza giornaliera.

Seguire le regole di protezione di base

Questa è la regola più utile e più efficace di tutte: essere sempre prudenti. Oggi, molte infiltrazioni richiedono l'intervento dell'utente affinché possano essere eseguite e distribuite. Adottando un comportamento prudente all'apertura di nuovi file, non sarà più necessario perdere tempo ed energie per pulire le infiltrazioni. Seguono alcune linee guida utili:

- Non visitare siti Web sospetti, con molte finestre popup e pubblicità che attirano l'attenzione.
- Prestare attenzione durante l'installazione di programmi freeware, pacchetti codec e così via. Utilizzare solo programmi sicuri e visitare solo siti Web Internet sicuri.
- Essere prudenti quando si aprono gli allegati e-mail, in particolare quelli inviati da programmi massmailer a destinatari multipli e quelli inviati da mittenti sconosciuti.
- Non utilizzare un account Amministratore per eseguire le attività quotidiane sul computer.

2. Installazione

Esistono vari metodi di installazione di ESET NOD32 Antivirus sul computer. I metodi di installazione possono variare in base al Paese e ai mezzi di distribuzione:

- Live installer può essere scaricato dal sito Web ESET. Il pacchetto di installazione è universale per tutte le lingue (scegliere la lingua desiderata). Di per sé, il Live installer è un file di piccole dimensioni; i file aggiuntivi necessari per l'installazione di ESET NOD32 Antivirus verranno scaricati automaticamente.

- Installazione off-line - Questo tipo di installazione viene utilizzato per le installazioni mediante il CD/DVD di un prodotto. Questa installazione utilizza un file *.msi* più grande rispetto al file Live installer e non richiede una connessione a Internet o file aggiuntivi per il completamento del processo.

Importante: Verificare che nel computer non siano installati altri programmi antivirus prima dell'installazione di ESET NOD32 Antivirus. Se su un singolo computer sono installate due o più soluzioni antivirus, potrebbero entrare in conflitto tra loro. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema. Per un elenco degli strumenti di disinstallazione dei software antivirus comuni, consultare l'articolo della Knowledge Base ESET (disponibile in inglese e in altre lingue).

2.1 Live installer

Dopo aver scaricato il pacchetto di installazione *Live installer*, fare doppio clic sul file di installazione e seguire le istruzioni dettagliate nella finestra del programma di installazione.

Importante: per questo tipo di installazione, è necessario effettuare la connessione a Internet.

NOD32 ANTIVIRUS 9
Installa ESET NOD32 Antivirus
Una soluzione antivirus rapida e potente
Naviga, gioca e connettiti in modo più sicuro grazie alle opzioni rapide ed efficaci offerte da ESET NOD32 Antivirus. La soluzione è in grado di eliminare un'ampia gamma di minacce presenti su Internet.
Continua
Italiano

Selezionare la lingua desiderata dal menu a discesa e fare clic su **Avanti**. Attendere alcuni istanti per il download dei file di installazione.

Dopo aver accettato l'**Accordo di licenza per l'utente finale**, verrà richiesto di configurare **ESET LiveGrid®**. ESET LiveGrid® garantisce un aggiornamento tempestivo e ininterrotto di ESET sulle nuove minacce al fine di garantire la protezione di tutti gli utenti. Il sistema consente l'invio di nuove minacce al laboratorio di ricerca ESET, dove i virus verranno analizzati, elaborati e aggiunti al database delle firme antivirali.

Per impostazione predefinita, l'opzione **Desidero partecipare a ESET LiveGrid® (scelta consigliata)** è selezionata e tale funzionalità sarà quindi attivata.

Il passaggio successivo del processo di installazione consiste nella configurazione dell'opzione di rilevamento delle applicazioni potenzialmente indesiderate. Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Per ulteriori informazioni, consultare il capitolo Applicazioni potenzialmente indesiderate.

Fare clic su **Installa** per avviare il processo di installazione.

2.2 Installazione off-line

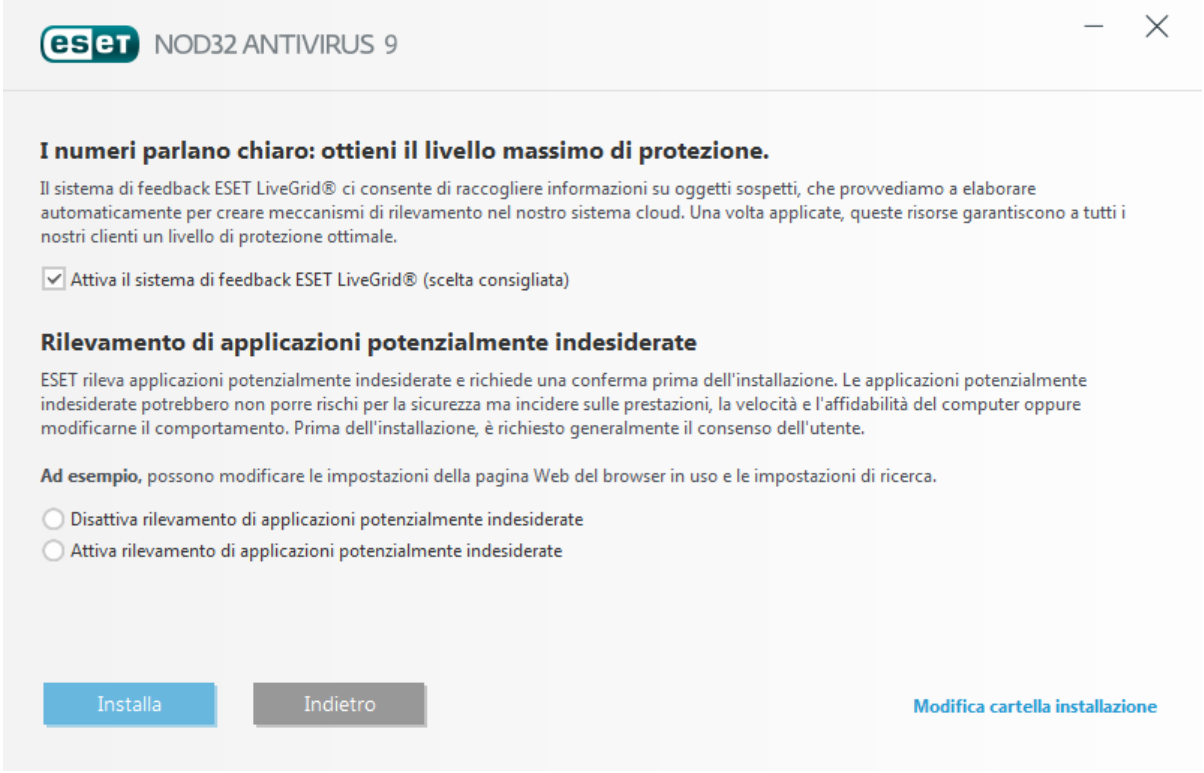
Dopo aver avviato il pacchetto di installazione off-line (.msi), la procedura di installazione guidata condurrà l'utente attraverso il processo di configurazione.

NOD32 ANTIVIRUS 9
Installa ESET NOD32 Antivirus
Una soluzione antivirus rapida e potente
Naviga, gioca e connettiti in modo più sicuro grazie alle opzioni rapide ed efficaci offerte da ESET NOD32 Antivirus. La soluzione è in grado di eliminare un'ampia gamma di minacce presenti su Internet.
9.0.303.1
Continua

Il programma controlla innanzitutto se è disponibile una versione più recente di ESET NOD32 Antivirus. Se è disponibile una versione più recente, ciò verrà segnalato all'utente durante il primo passaggio del processo di installazione. Se si seleziona **Scarica e installa la nuova versione**, verrà scaricata la nuova versione e sarà possibile proseguire con l'installazione. La casella di controllo è visibile solo in caso di disponibilità di una versione più recente rispetto a quella installata dall'utente.

Successivamente, verrà visualizzato l'Accordo di licenza per l'utente finale. Si prega di leggere l'accordo e di fare clic su **Accetto** per confermare l'accettazione dei termini dell'Accordo di licenza per l'utente finale. Dopo aver accettato, l'installazione procederà.

Per ulteriori informazioni sui passaggi di installazione, **ThreatSense** e **Rilevamento di applicazioni potenzialmente indesiderate**, seguire le istruzioni nella sezione precedente (vedere "Live installer").


NOD32 ANTIVIRUS 9
I numeri parlano chiaro: ottieni il livello massimo di protezione.
Il sistema di feedback ESET LiveGrid® ci consente di raccogliere informazioni su oggetti sospetti, che provvediamo a elaborare automaticamente per creare meccanismi di rilevamento nel nostro sistema cloud. Una volta applicate, queste risorse garantiscono a tutti i nostri clienti un livello di protezione ottimale.
Attiva il sistema di feedback ESET LiveGrid® (scelta consigliata)
Rilevamento di applicazioni potenzialmente indesiderate
ESET rileva applicazioni potenzialmente indesiderate e richiede una conferma prima dell'installazione. Le applicazioni potenzialmente indesiderate potrebbero non porre rischi per la sicurezza ma incidere sulle prestazioni, la velocità e l'affidabilità del computer oppure modificarne il comportamento. Prima dell'installazione, è richiesto generalmente il consenso dell'utente.
Ad esempio, possono modificare le impostazioni della pagina Web del browser in uso e le impostazioni di ricerca.
Disattiva rilevamento di applicazioni potenzialmente indesiderate
Attiva rilevamento di applicazioni potenzialmente indesiderate
Installa
Indietro
Modifica cartella installazione

2.2.1 Impostazioni avanzate

Dopo aver selezionato **Impostazioni avanzate**, all'utente verrà richiesto di selezionare un percorso per l'installazione. Per impostazione predefinita, il programma viene installato nella directory seguente:

C:\Programmi\ESET\ESET NOD32 Antivirus

Scegliere **Sfoglia...** per selezionare un percorso diverso (scelta non consigliata).

Fare clic su **Avanti** per configurare la connessione a Internet. Se si utilizza un server proxy, è necessario configurarlo correttamente per l'esecuzione degli aggiornamenti delle firme antivirali. Se non si è sicuri se si sta utilizzando un server proxy per la connessione a Internet, selezionare **Utilizzo le stesse impostazioni di Internet Explorer (scelta consigliata)** e fare clic su **Avanti**. Se non si utilizza un server proxy, selezionare **Non utilizzo un server proxy**.

Per configurare le impostazioni del server proxy, selezionare **Viene utilizzato un server proxy**, quindi fare clic su **Avanti**. Immettere l'indirizzo IP o l'URL del server proxy nel campo **Indirizzo**. Nel campo **Porta** specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Nel caso in cui il server proxy richieda l'autenticazione, sarà necessario immettere un **Nome utente** e **Password** validi per consentire l'accesso al server proxy. Se si desidera è anche possibile copiare le impostazioni del server proxy da Internet Explorer.. A tale scopo, fare clic su **Applica** e confermare la selezione.

L'installazione personalizzata consente all'utente di definire le modalità di gestione degli aggiornamenti automatici del programma sul sistema. Fare clic su **Modifica...** per accedere alle Impostazioni avanzate.

Se non si desidera aggiornare i componenti di programma, selezionare **Non aggiornare mai i componenti di programma**. Selezionare **Chiedi prima di scaricare i componenti di programma** per visualizzare una finestra di conferma ogni volta che il sistema tenta di scaricare i componenti di programma. Per scaricare automaticamente gli upgrade dei componenti di programma, selezionare **Aggiorna sempre i componenti di programma**.

NOTA: in genere, dopo aver aggiornato un componente di programma, è necessario riavviare il sistema. Si consiglia di selezionare **Se necessario, riavvia il computer senza notifica**.

Nella finestra di installazione successiva è disponibile l'opzione per impostare una password per proteggere le impostazioni del programma. Selezionare **Proteggi le impostazioni di configurazione con password** e inserire la password nei campi **Nuova password** e **Conferma nuova password**. Questa password verrà richiesta per modificare o accedere alle impostazioni di ESET NOD32 Antivirus. Se i campi delle password corrispondono, fare clic su **Avanti** per continuare.

Per completare i successivi passaggi di installazione, **ThreatSense** e **Rilevamento di applicazioni potenzialmente indesiderate**, seguire le istruzioni nella sezione Live installer (vedere "Live installer").

Per disattivare il primo controllo dopo l'installazione, eseguito normalmente al termine dell'installazione ai fini della ricerca di codice dannoso, deselezionare la casella di controllo accanto a **Attiva controllo dopo l'installazione**. Fare clic su **Installa** nella finestra **Pronto all'installazione** per completare l'installazione.

2.3 Problemi di installazione comuni

Se durante l'installazione si verificano problemi, consultare l'elenco di errori di installazione comuni e risoluzioni per trovare una soluzione al problema.

2.4 Attivazione prodotto

Al termine dell'installazione, all'utente verrà richiesto di attivare il prodotto.

Sono disponibili vari metodi per attivare il prodotto. La disponibilità di uno scenario di attivazione specifico nella finestra di attivazione potrebbe variare in base al Paese e ai mezzi di distribuzione (CD/DVD, pagina Web ESET, ecc.).

- Se è stata acquistata una versione presso un rivenditore al dettaglio del prodotto, attivare il prodotto tramite una **Chiave di licenza**. La chiave di licenza si trova generalmente all'interno o sul retro della confezione del prodotto. Per eseguire correttamente l'attivazione, è necessario inserire la chiave di licenza così come fornita. Chiave di licenza: stringa univoca nel formato XXXX-XXXX-XXXX-XXXX-XXXX o XXXX-XXXXXXXX, utilizzata per l'identificazione del proprietario della licenza e per l'attivazione della licenza.
- Se si desidera provare ESET NOD32 Antivirus prima di acquistarlo, selezionare **Licenza di prova gratuita**. Inserire l'indirizzo e-mail e il Paese per attivare ESET NOD32 Antivirus per un periodo di tempo limitato. La licenza di prova verrà inviata all'indirizzo indicato dall'utente. È possibile attivare una sola licenza di prova per cliente.
- Qualora non si disponga di una licenza e si desideri acquistarne una, fare clic su Acquista licenza. In tal modo si verrà reindirizzati al sito Web o al distributore locale ESET.

Selezionare **Attiva in seguito** se si desidera valutare rapidamente il prodotto e non attivarlo immediatamente o se si desidera attivarlo in seguito.

È inoltre possibile attivare una copia di ESET NOD32 Antivirus direttamente dal programma. Fare clic con il pulsante destro del mouse sull'icona ESET NOD32 Antivirus sulla barra delle applicazioni e selezionare **Attiva prodotto** dal Menu del programma.

2.5 Inserimento della chiave di licenza

Per garantire una funzionalità ottimale è fondamentale che il programma venga aggiornato automaticamente. Ciò è possibile solo inserendo la **Chiave di licenza** corretta nella **Configurazione dell'aggiornamento**.

Nel caso in cui la chiave di licenza non sia stata immessa durante l'installazione, è possibile inserirla ora. Nella finestra principale del programma, fare clic su **Guida e supporto tecnico**, quindi selezionare **Attiva licenza** e inserire i dati di licenza ricevuti insieme al prodotto di protezione ESET nella finestra Attivazione prodotto.

Quando si immette la **Chiave di licenza**, è importante immetterla esattamente come è scritta:

- Una stringa univoca nel formato XXXX-XXXX-XXXX-XXXX-XXXX, utilizzata per l'identificazione del proprietario della licenza e per l'attivazione della stessa.

Per evitare errori, si consiglia di copiare e incollare la chiave di licenza dal messaggio e-mail di registrazione.

2.6 Aggiornamento a una versione più recente

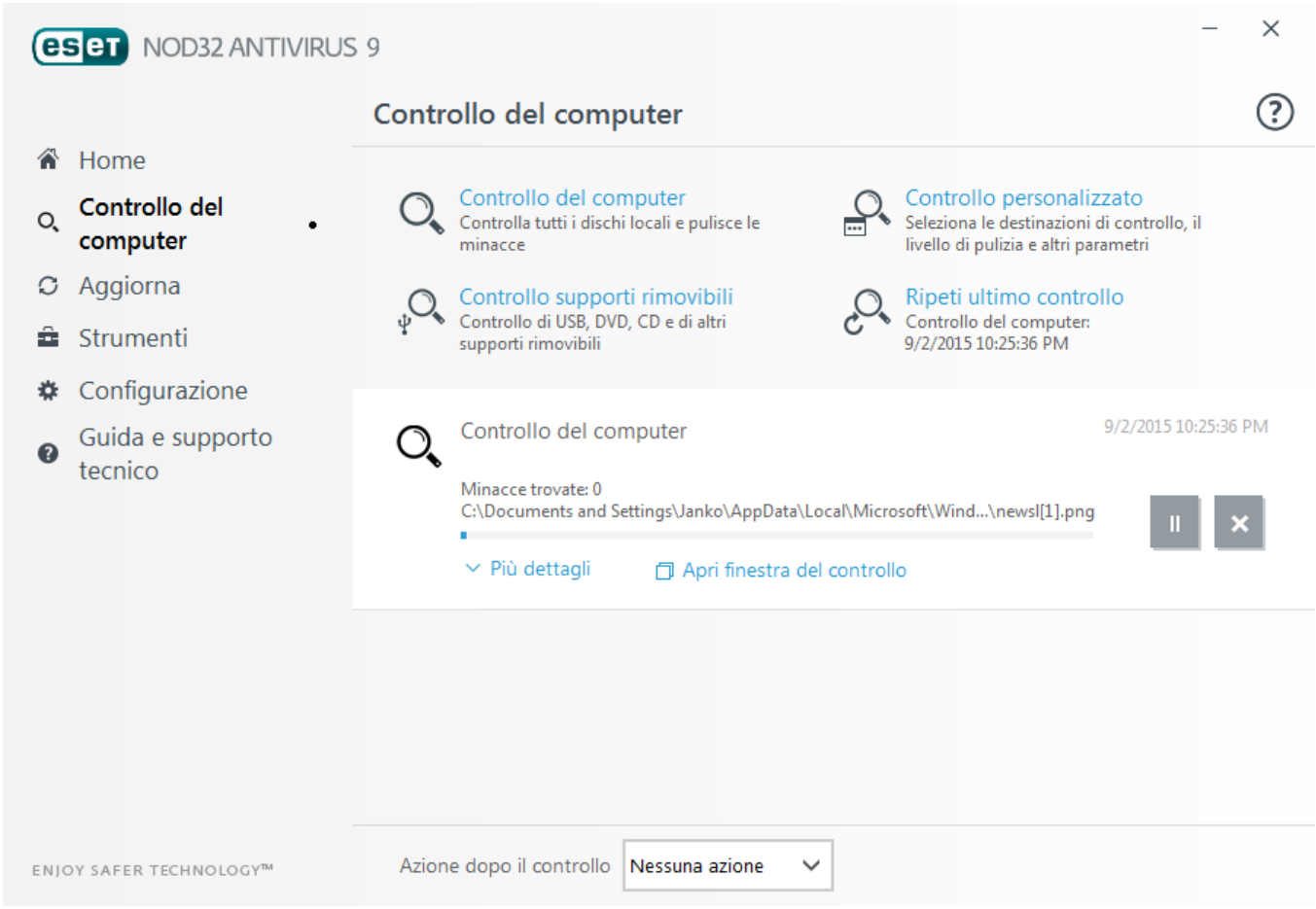
Le nuove versioni di ESET NOD32 Antivirus vengono rilasciate ai fini dell'implementazione di miglioramenti o della correzione di errori che non è possibile risolvere mediante aggiornamenti automatici dei moduli del programma. L'aggiornamento a una versione più recente può essere eseguito in diversi modi:

1. Automaticamente tramite un aggiornamento del programma.
   L'upgrade del programma, che viene distribuito a tutti gli utenti e che potrebbe incidere su alcune configurazioni di sistema, viene rilasciato dopo un lungo periodo di prova per garantire un livello di compatibilità massimo. Se è necessario eseguire l'aggiornamento a una versione più recente nel momento in cui viene rilasciato, usare uno dei metodi seguenti.
2. Manualmente nella finestra principale del programma selezionando **Verifica aggiornamenti** nella sezione **Aggiorna**.
3. Manualmente scaricando e installando una versione più recente su quella precedente.

2.7 Primo controllo dopo l'installazione

Dopo aver installato ESET NOD32 Antivirus, verrà avviato un controllo del computer 20 minuti dopo l'installazione o il riavvio del computer ai fini della ricerca di codice dannoso.

È inoltre possibile avviare manualmente un controllo del computer dalla finestra principale del programma facendo clic su **Controllo del computer** > **Controlla il computer in uso**. Per ulteriori informazioni sui controlli del computer, consultare la sezione Controllo del computer.



3. Guida introduttiva

In questo capitolo viene fornita una panoramica su ESET NOD32 Antivirus e sulle configurazioni di base.

3.1 La finestra principale del programma

La finestra principale di ESET NOD32 Antivirus è suddivisa in due sezioni principali. La finestra principale sulla destra contiene informazioni corrispondenti all'opzione selezionata dal menu principale sulla sinistra.

Di seguito è riportata una descrizione delle opzioni del menu principale:

Stato protezione - Fornisce informazioni relative allo stato di protezione di ESET NOD32 Antivirus.

Controllo computer: consente di configurare e avviare un controllo del computer o di creare un controllo personalizzato.

Aggiorna - Consente di visualizzare informazioni relative agli aggiornamenti del database delle firme antivirali.

Strumenti - Consente di accedere ai File di rapporto, Statistiche di protezione, Attività di verifica, Processi in esecuzione, Pianificazione attività, ESET SysInspector e ESET SysRescue.

Configurazione: selezionare questa opzione per regolare il livello di protezione per Computer, Internet.

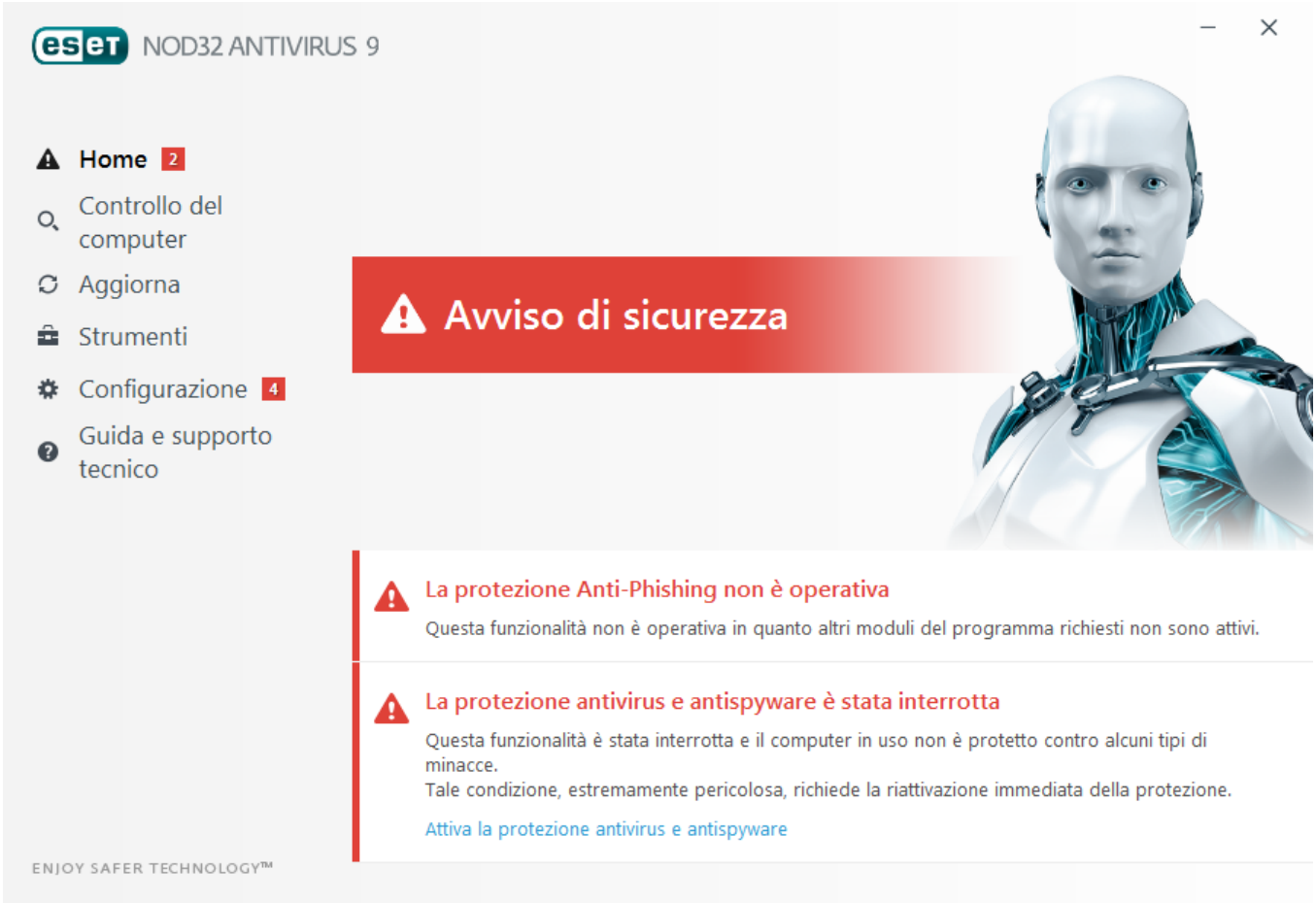
Guida e supporto tecnico: consente di accedere ai file della Guida, alla Knowledge Base ESET, al sito Web ESET e ai collegamenti per inviare una richiesta di assistenza.

Nella schermata **Home** vengono visualizzate informazioni importanti sul livello di protezione corrente del computer in uso. Nella finestra di stato sono visualizzate le funzionalità di ESET NOD32 Antivirus usate più frequentemente. In questa finestra sono inoltre visualizzate le informazioni sull'aggiornamento più recente e la data di scadenza del programma.

L'icona verde e il colore verde dello stato **Protezione massima** indicano un livello di protezione massimo.

Cosa fare se il programma non funziona correttamente?

Se un modulo di protezione attivo funziona correttamente, la relativa icona dello stato di protezione sarà verde. Un punto esclamativo rosso o un'icona di notifica arancione indica che non è garantito il livello massimo di protezione. In **Home** verranno visualizzate informazioni aggiuntive sullo stato di protezione di ciascun modulo, nonché le soluzioni consigliate per il ripristino della protezione completa. Per modificare lo stato dei singoli moduli, fare clic su **Configurazione** e selezionare il modulo desiderato.


NOD32 ANTIVIRUS 9
Home 2
Controllo del computer
Aggiorna
Strumenti
Configurazione 4
Guida e supporto tecnico
Avviso di sicurezza
La protezione Anti-Phishing non è operativa
Questa funzionalità non è operativa in quanto altri moduli del programma richiesti non sono attivi.
La protezione antivirus e antispyware è stata interrotta
Questa funzionalità è stata interrotta e il computer in uso non è protetto contro alcuni tipi di minacce.
Tale condizione, estremamente pericolosa, richiede la riattivazione immediata della protezione.
Attiva la protezione antivirus e antispyware
ENJOY SAFER TECHNOLOGY™

L'icona rossa e il colore rosso della sezione Home indicano la presenza di problemi critici da parte dello stato. Esistono vari motivi alla base della visualizzazione di questo stato, tra cui:

- **Prodotto non attivato** - È possibile attivare ESET NOD32 Antivirus da **Home** facendo clic su **Attiva prodotto** o **Acquista ora** in Stato protezione.
- **Il database delle firme antivirali è obsoleto** - Questo errore viene visualizzato dopo diversi tentativi non riusciti di aggiornamento del database delle firme antivirali. Si consiglia di controllare le impostazioni di aggiornamento. I motivi più comuni alla base di questo errore consistono in un inserimento errato dei dati di autenticazione o in una configurazione non corretta delle impostazioni di connessione.
- **Protezione antivirus e antispyware disattivata** - È possibile riattivare la protezione antivirus e antispyware facendo clic su **Avvia tutti i moduli di protezione antivirus e antispyware**.
- **Licenza scaduta** - Questa condizione è indicata dalla presenza di un'icona rossa dello stato di protezione. Allo scadere della licenza, non sarà possibile aggiornare il programma. Seguire le istruzioni nella finestra di avviso per rinnovare la licenza.

L'icona arancione indica una protezione limitata. Ad esempio, potrebbe essersi verificato un problema nell'aggiornamento del programma o la licenza potrebbe essere in fase di scadenza.
Esistono vari motivi alla base della visualizzazione di questo stato, tra cui:

- **Modalità giocatore attivata** - L'attivazione della Modalità giocatore è un potenziale rischio di protezione. L'attivazione di questa funzionalità disattiva tutte le finestre popup e interrompe qualsiasi attività pianificata.

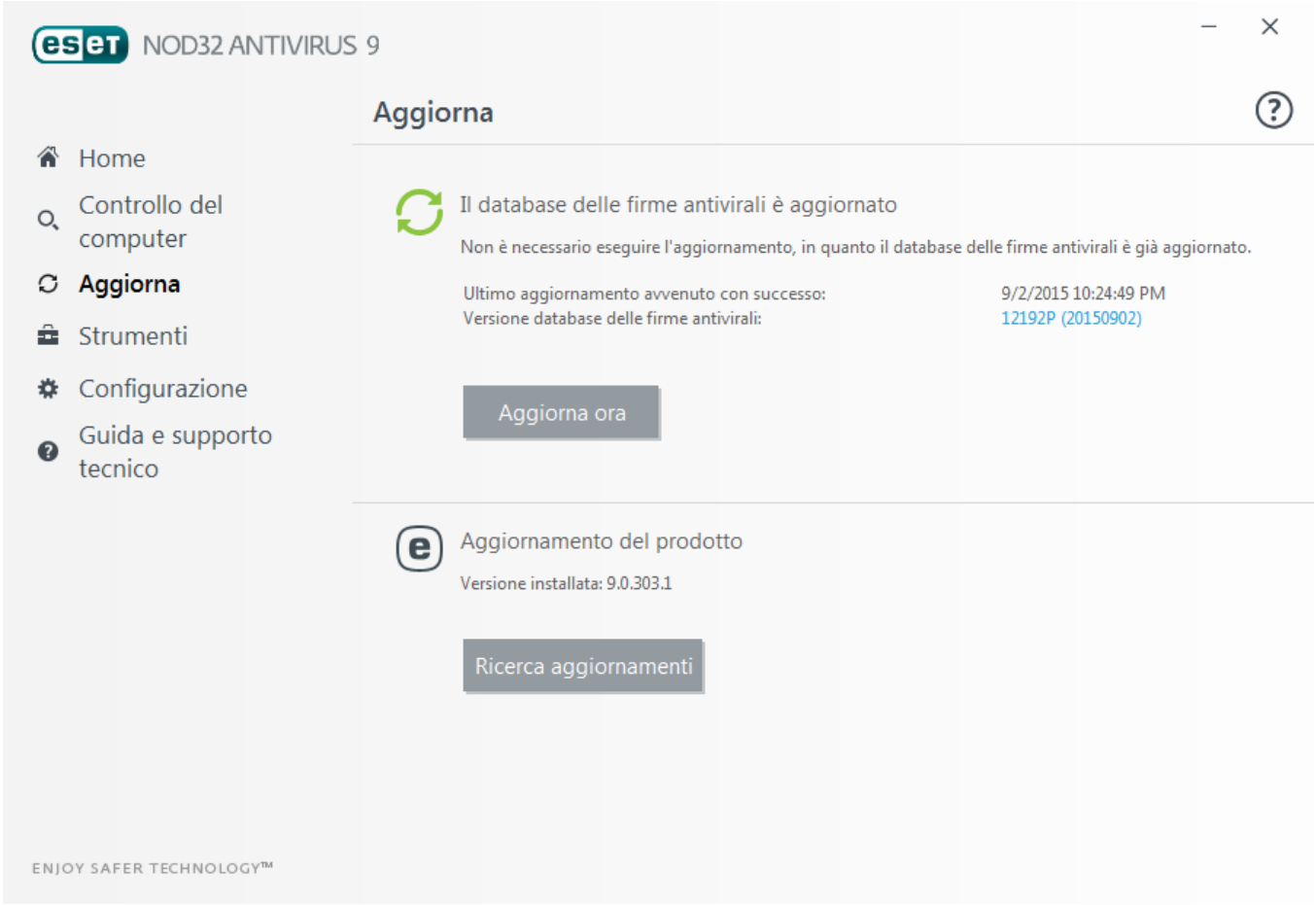
- **La licenza scadrà a breve** - Questa condizione è indicata dalla presenza di un'icona dello stato di protezione contenente un punto esclamativo vicino all'orologio di sistema. Allo scadere della licenza, non sarà possibile aggiornare il programma e l'icona dello stato di protezione diventerà rossa.

Qualora non si riuscisse a risolvere un problema ricorrendo alle soluzioni consigliate, fare clic su **Guida e supporto tecnico** per accedere ai file della Guida oppure effettuare una ricerca nella Knowledge Base ESET. Per ulteriore assistenza, è possibile inviare una richiesta di supporto. Il Supporto tecnico ESET risponderà rapidamente alle domande degli utenti e li aiuterà a trovare una soluzione ai loro problemi.

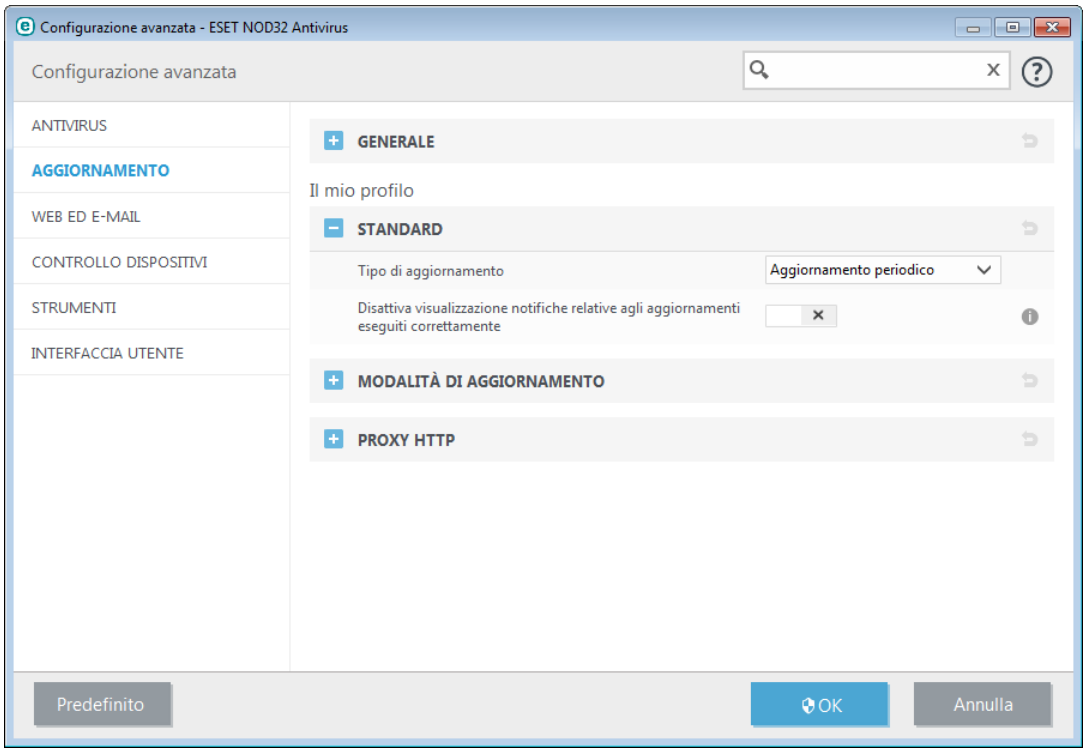
3.2 Aggiornamenti

L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per garantire la protezione del sistema contro codici dannosi. È opportuno prestare particolare attenzione alla relativa configurazione e al funzionamento. Nel menu principale, fare clic su **Aggiorna**, quindi su **Aggiorna adesso** per verificare la disponibilità di un aggiornamento del database delle firme antivirali.

Se durante l'attivazione di ESET NOD32 Antivirus non sono stati specificati Nome utente e Password, verrà richiesto di inserirli in questa fase.

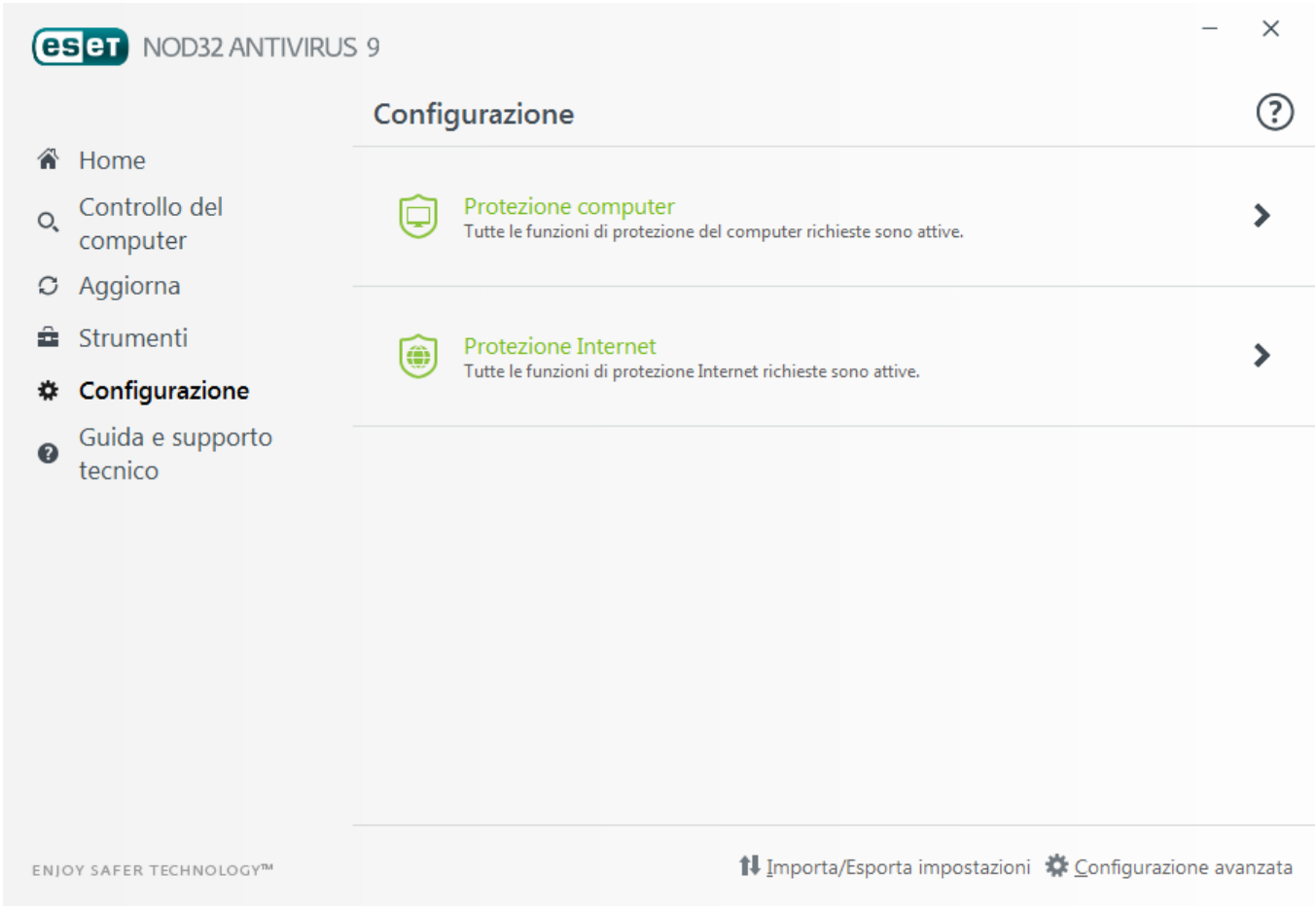


Nella finestra Configurazione avanzata (fare clic su **Configurazione** nel menu principale, quindi su **Configurazione avanzata** oppure premere **F5** sulla tastiera), sono disponibili ulteriori opzioni di aggiornamento. Per configurare le opzioni di aggiornamento avanzate, come ad esempio la modalità di aggiornamento, l'accesso al server proxy e le connessioni LAN, fare clic sulla scheda specifica nella finestra **Aggiornamento**.



4. Utilizzo di ESET NOD32 Antivirus

Le opzioni di configurazione di ESET NOD32 Antivirus consentono di regolare i livelli di protezione del computer.



Il menu **Configurazione** è suddiviso nelle seguenti sezioni:

Protezione del computer

Protezione Internet

Fare clic su un componente per regolare le impostazioni avanzate del modulo di protezione corrispondente.

L'impostazione della **Protezione computer** consente di attivare o disattivare i componenti seguenti:

- **Protezione file system in tempo reale**: tutti i file vengono sottoposti a controllo per la ricerca di codici dannosi al momento dell'apertura, creazione o esecuzione sul computer.
- **HIPS** - Il sistema HIPS monitora gli eventi all'interno del sistema operativo e reagisce in base a una serie personalizzata di regole.
- **Modalità giocatore** - Attiva o disattiva la Modalità giocatore. Quando si attiva la Modalità giocatore, viene visualizzato un messaggio di avviso (potenziale rischio per la protezione) e la finestra principale diventa arancione.

L'impostazione della **Protezione Internet** consente di attivare o disattivare i componenti seguenti:

- **Protezione accesso Web** - Se questa opzione è attivata, viene eseguito il controllo di tutto il traffico HTTP o HTTPS per la ricerca di software dannoso.
- **Protezione client di posta** - Monitora le comunicazioni ricevute mediante il protocollo POP3 e IMAP.
- **Protezione Anti-Phishing**: filtra i siti Web per i quali si sospetta una distribuzione di contenuti concepiti allo scopo di manipolare gli utenti facendo loro inviare informazioni riservate.

Per riattivare un componente di protezione disattivato, fare clic sul cursore affinché sia visualizzato un

segno di spunta verde .

NOTA: quando si disattiva la protezione mediante questo metodo, tutti i moduli di protezione disattivati saranno attivati dopo aver riavviato il computer.

Nella parte inferiore della finestra di configurazione sono disponibili ulteriori opzioni. Utilizzare il collegamento **Configurazione avanzata** per configurare parametri più dettagliati per ciascun modulo. Utilizzare **Importa/esporta impostazioni** per caricare i parametri di configurazione mediante un file di configurazione *.xml* o per salvare i parametri di configurazione correnti in un file di configurazione.

4.1 Protezione del computer

Fare clic su Protezione del computer nella finestra Configurazione per visualizzare una panoramica di tutti i moduli di protezione. Per disattivare temporaneamente i singoli moduli, fare clic su . Tenere presente che in questo modo si potrebbe ridurre il livello di protezione del computer. Fare clic su accanto a un modulo di protezione per accedere alle impostazioni avanzate di tale modulo.

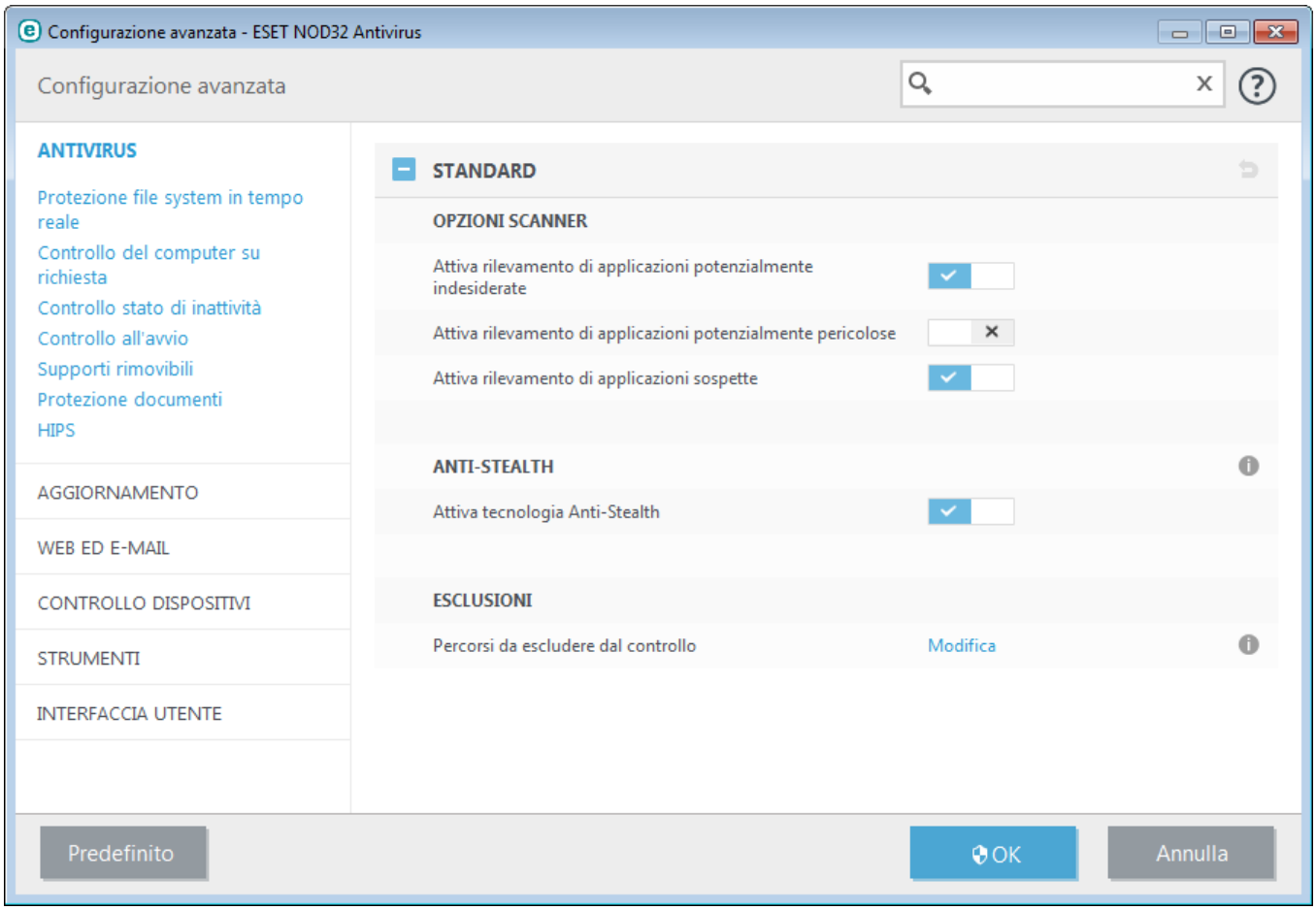
Fare clic su > **Modifica esclusioni** accanto a **Protezione file system in tempo reale** per aprire la finestra di configurazione Esclusioni che consente all'utente di escludere file e cartelle dal controllo.

NOD32 ANTIVIRUS 9
Protezione computer
Home
Controllo del computer
Aggiorna
Strumenti
Configurazione
Guida e supporto tecnico
Protezione file system in tempo reale
Attivata: rilevamento e pulizia immediati di malware sul computer in uso.
Host Intrusion Prevention System (HIPS)
Attivato: rilevamento e prevenzione di comportamenti indesiderati da parte delle applicazioni.
Modalità giocatore
Interrotta: ottimizzazione delle prestazioni per giochi e presentazioni.
Sospendi la protezione antivirus e antispyware
ENJOY SAFER TECHNOLOGY™
Importa/Esporta impostazioni
Configurazione avanzata

Sospendi la protezione antivirus e antispyware: disattiva tutti i moduli di protezione antivirus e antispyware. Una volta disattivata la protezione, comparirà una finestra che consente all'utente di determinare la durata della disattivazione della protezione mediante il menu a discesa **Intervallo di tempo**. Fare clic su **OK** per confermare.

4.1.1 Antivirus

La protezione antivirus difende il sistema da attacchi dannosi controllando file, e-mail e comunicazioni su Internet. Il modulo antivirus è in grado di eliminare una minaccia con codice dannoso rilevata. L'oggetto viene dapprima bloccato, poi pulito, cancellato o messo in quarantena.



Le **opzioni scanner** per tutti i moduli di protezione (ad esempio, protezione file system in tempo reale, protezione accesso Web, ecc.) consentono di attivare o disattivare il rilevamento dei seguenti elementi:

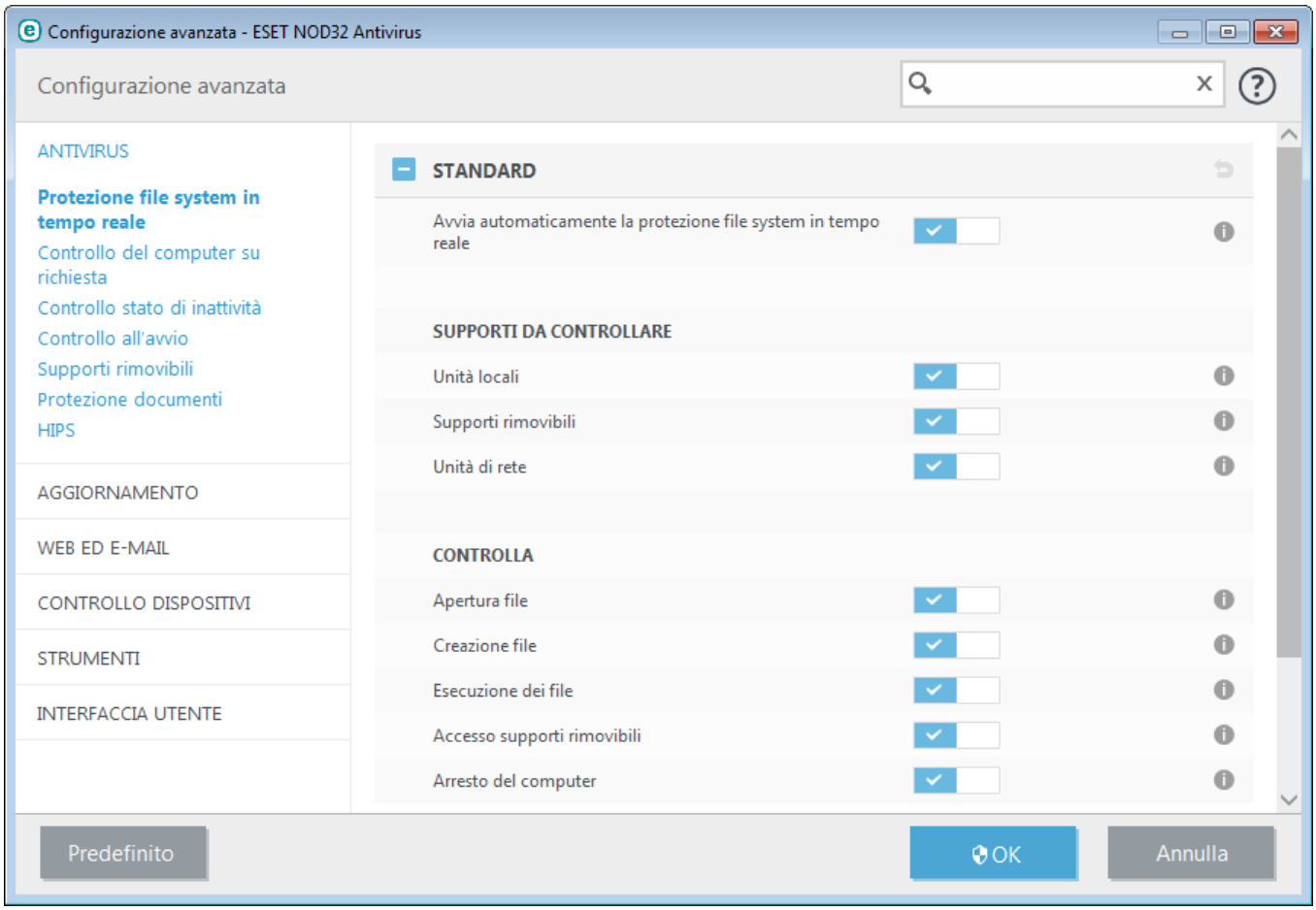
- Le **Applicazioni potenzialmente indesiderate** (PUA) non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso.
  Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.
- Le **Applicazioni potenzialmente pericolose** sono software legali e commerciali che potrebbero essere utilizzati in modo non legale per scopi illegittimi. Esempi di applicazioni potenzialmente pericolose sono strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente). Questa opzione è disattivata per impostazione predefinita.
  Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.
- Le **Applicazioni sospette** includono programmi compressi mediante programmi di compressione o protettori. Questi tipi di programmi di protezione sono spesso utilizzati dagli autori di malware per eludere il rilevamento.

La **tecnologia Anti-Stealth** è un sistema sofisticato che consente di rilevare programmi pericolosi, come ad esempio i rootkit, che sono in grado di nascondersi dal sistema operativo. Ciò significa che non è possibile rilevarli utilizzando le normali tecnologie di testing.

Le **Esclusioni** consentono all'utente di escludere file e cartelle dal controllo. Per garantire che la ricerca delle minacce venga eseguita su tutti gli oggetti, si consiglia di creare esclusioni solo se assolutamente necessario. Le situazioni in cui potrebbe essere necessario escludere un oggetto potrebbero includere, ad esempio, il controllo di voci di database di grandi dimensioni che rallenterebbero il computer durante un controllo o di un software che entra in conflitto con il controllo. Per escludere un oggetto dal controllo, consultare il paragrafo Esclusioni.

4.1.1.1 Protezione file system in tempo reale

La funzione di Protezione file system in tempo reale consente di controllare tutti gli eventi correlati all'antivirus nel sistema. Su tutti i file vengono ricercati codici dannosi al momento dell'apertura, creazione o esecuzione sul computer. La funzione Protezione file system in tempo reale viene avviata all'avvio del sistema.



Per impostazione predefinita, la Protezione file system in tempo reale viene avviata all'avvio del sistema e fornisce un controllo ininterrotto. In casi particolari (ad esempio, in caso di conflitto con un altro scanner in tempo reale), la Protezione in tempo reale può essere disattivata deselezionando **Avvia automaticamente la protezione file system in tempo reale** in **Configurazione avanzata** sotto a **Protezione file system in tempo reale** > **Di base**.

Supporti da controllare

Per impostazione predefinita, vengono controllati tutti i tipi di supporto alla ricerca di eventuali minacce:

Dischi locali - Consente di controllare tutti gli hard disk del sistema.
Supporti rimovibili: consente di controllare CD/DVD, supporti di archiviazione USB, dispositivi Bluetooth e così via.
Dischi di rete - Consente di eseguire il controllo di tutte le unità mappate.

Si consiglia di utilizzare le impostazioni predefinite e di modificarle solo in casi specifici, ad esempio quando il controllo di alcuni supporti rallenta notevolmente il trasferimento dei dati.

Controlla

Per impostazione predefinita, tutti i file vengono controllati al momento dell'apertura, creazione o esecuzione. Si consiglia di mantenere le seguenti impostazioni predefinite per garantire il massimo livello di protezione in tempo reale per il computer in uso:

- **Apertura dei file**: attiva o disattiva il controllo al momento dell'apertura dei file.
- **Creazione dei file**: attiva o disattiva il controllo al momento della creazione dei file.
- **Esecuzione dei file**: attiva o disattiva il controllo al momento dell'esecuzione dei file.
- **Accesso supporti rimovibili** - Attiva o disattiva il controllo attivato dall'accesso a determinati supporti rimovibili dotati di uno spazio di archiviazione.
- **Arresto computer**: attiva o disattiva il controllo attivato dall'arresto del computer.

La Protezione file system in tempo reale, che viene attivata da vari eventi di sistema, tra cui l'accesso a un file, controlla tutti i tipi di supporti. Grazie ai metodi di rilevamento della tecnologia ThreatSense (descritti nella sezione Configurazione parametri motore ThreatSense), è possibile configurare la Protezione file system in tempo reale allo scopo di gestire i file di nuova creazione in base a modalità diverse rispetto a quelle utilizzate per i file esistenti. Ad esempio, la Protezione file system in tempo reale può essere configurata in modo da monitorare più da vicino i file di nuova creazione.

Per ridurre al minimo l'impatto sul sistema della protezione in tempo reale, i file che sono già stati controllati verranno ignorati, eccetto nel caso in cui siano state apportate modifiche. I file vengono controllati nuovamente subito dopo ogni aggiornamento del database delle firme antivirali. Questo comportamento viene controllato mediante l'utilizzo dell'**Ottimizzazione intelligente**. Se l'**Ottimizzazione intelligente** è disattivata, tutti i file verranno controllati a ogni accesso. Per modificare questa impostazione, premere **F5** per aprire Configurazione avanzata ed espandere **Antivirus** > **Protezione file system in tempo reale**. Fare clic su **parametro ThreatSense** > **Altro** e selezionare o deselezionare **Attiva ottimizzazione intelligente**.

4.1.1.1.1 Parametri ThreatSense aggiuntivi

Parametri ThreatSense aggiuntivi per i file appena creati e modificati

I file appena creati o modificati hanno maggiore possibilità di essere infettati rispetto a quelli esistenti. Per tale motivo, il programma controlla tali file con parametri di controllo aggiuntivi. ESET NOD32 Antivirus utilizza la funzione di euristica avanzata che è in grado di rilevare le nuove minacce prima del rilascio dell'aggiornamento del database delle firme antivirali insieme a metodi di controllo basati sulle firme. Oltre che sui file appena creati, il controllo viene eseguito anche sugli **Archivi autoestraenti** (SFX) e sugli **Eseguibili compressi** (file eseguibili compressi a livello interno). Per impostazione predefinita, gli archivi vengono analizzati fino al 10° livello di nidificazione e controllati indipendentemente dalla loro dimensione effettiva. Per modificare le impostazioni di controllo dell'archivio, deselezionare **Impostazioni predefinite controllo degli archivi**.

Parametri ThreatSense aggiuntivi per i file eseguiti

Euristica avanzata all'esecuzione dei file - Per impostazione predefinita, all'esecuzione dei file viene utilizzata l'Euristica avanzata. Una volta attivata, si consiglia vivamente di mantenere attivi l'Ottimizzazione intelligente ed ESET LiveGrid®, allo scopo di ridurre l'impatto sulle prestazioni del sistema.

Euristica avanzata all'esecuzione dei file da supporti rimovibili - L'euristica avanzata emula il codice in un ambiente virtuale e ne valuta il comportamento prima che venga consentita l'esecuzione da supporti rimovibili.

4.1.1.1.2 Livelli di pulizia

La protezione in tempo reale prevede tre livelli di pulizia (per accedere alle impostazioni dei livelli di pulizia, fare clic su **Configurazione parametri motore ThreatSense** nella sezione **Protezione file system in tempo reale**, quindi su **Pulizia**).

Nessuna pulizia - I file infetti non vengono puliti automaticamente. Verrà visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione. Questo livello è indicato per utenti più esperti in grado di eseguire le azioni appropriate in caso di infiltrazione.

Pulitura standard - Il programma tenterà di pulire o eliminare automaticamente un file infetto in base a un'azione predefinita (a seconda del tipo di infiltrazione). Una notifica nell'angolo in basso a destra della schermata segnalerà il rilevamento e l'eliminazione di un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma offre altre azioni di follow-up. Lo stesso si verifica se non è stato possibile completare un'azione predefinita.

Massima pulizia - Il programma pulirà o eliminerà tutti i file infetti. Le uniche eccezioni sono costituite dai file di sistema. Nel caso in cui non sia possibile pulirli, verrà visualizzata una finestra di avviso con la possibilità di scegliere un'azione da eseguire.

Attenzione: se un archivio contiene uno o più file infetti, sono disponibili due opzioni per gestire tale archivio. In modalità standard (Pulitura standard), l'intero archivio viene eliminato se tutti i file in esso contenuti sono infetti. In modalità **Massima pulizia**, l'archivio viene eliminato se contiene almeno un file infetto, indipendentemente dallo stato degli altri file contenuti nell'archivio.

4.1.1.1.3 Quando modificare la configurazione della protezione in tempo reale

La protezione in tempo reale è il componente più importante per la sicurezza di un sistema. Prestare la massima attenzione quando si modificano i relativi parametri. È consigliabile modificarli solo in casi specifici.

Dopo aver installato ESET NOD32 Antivirus, tutte le impostazioni vengono ottimizzate al fine di offrire agli utenti il massimo livello di protezione del sistema. Per ripristinare le impostazioni predefinite, fare clic su ↩ accanto a ciascuna scheda nella finestra (**Configurazione avanzata** > **Antivirus** > **Protezione file system in tempo reale**).

4.1.1.1.4 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare un file di test da eicar.com. Questo file di test è un file innocuo e rilevabile da tutti i programmi antivirus. Il file è stato creato da EICAR (European Institute for Computer Antivirus Research) per testare la funzionalità dei programmi antivirus. Può essere scaricato all'indirizzo http://www.eicar.org/download/eicar.com

4.1.1.1.5 Cosa fare se la protezione in tempo reale non funziona

In questo capitolo, verranno illustrati i problemi che potrebbero verificarsi durante l'utilizzo della protezione in tempo reale e le modalità di risoluzione.

La protezione in tempo reale è disattivata

Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, selezionare **Configurazione** nella finestra principale del programma e fare clic su **Protezione del computer** > **Protezione file system in tempo reale**.

Se la protezione in tempo reale non viene lanciata all'avvio del sistema, è probabile che l'opzione **Avvia automaticamente la protezione file system in tempo reale** non sia selezionata. Per garantire che questa opzione sia attivata, accedere a Configurazione avanzata (**F5**) e fare clic su **Antivirus** > **Protezione file system in tempo reale**.

La protezione in tempo reale non rileva né pulisce le infiltrazioni

Verificare che nel computer non siano installati altri programmi antivirus. Se sono installate contemporaneamente due o più soluzioni antivirus, potrebbero entrare in conflitto tra loro. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema prima di installare ESET.

La protezione in tempo reale non viene avviata

Se la protezione in tempo reale non viene lanciata all'avvio del sistema (e l'opzione **Avvia automaticamente la protezione file system in tempo reale** è attivata), ciò potrebbe dipendere da un conflitto con altri programmi. Per ricevere assistenza nella risoluzione del problema, si prega di contattare il Supporto tecnico ESET.

4.1.1.2 Controllo del computer

Lo scanner su richiesta è una parte importante della soluzione antivirus. Viene utilizzato per eseguire il controllo di file e di cartelle sul computer in uso. Dal punto di vista della protezione, è essenziale che i controlli del computer non vengano eseguiti solo quando si sospetta un'infezione, ma periodicamente, nell'ambito delle normali misure di protezione. Si consiglia di eseguire periodicamente controlli approfonditi del sistema per rilevare virus non individuati dalla Protezione file system in tempo reale quando vengono scritti sul disco. Ciò può verificarsi se la protezione file system in tempo reale era disattivata in quel momento, il database antivirus era obsoleto o il file non è stato rilevato come virus nel momento in cui è stato salvato sul disco.

Sono disponibili due tipologie di **Controllo del computer**. **Controlla computer in uso** consente di controllare rapidamente il sistema senza dover specificare i parametri di controllo. **Controllo personalizzato**, che consente di selezionare uno dei profili di controllo predefiniti per l'analisi di percorsi specifici, nonché di scegliere specifiche destinazioni di controllo.

Controlla computer in uso

La funzione Controlla computer in uso consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio della funzione Controlla computer in uso consiste nella facilità di utilizzo e nel fatto che non è richiesta una configurazione di controllo dettagliata. Questo tipo di controllo consente di effettuare un controllo di tutti i file presenti nelle unità locali, nonché una pulizia o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di pulizia viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di pulizia, consultare il paragrafo Pulizia.

Controllo personalizzato

Il controllo personalizzato consente di specificare parametri di controllo quali destinazioni e metodi di controllo. Il vantaggio del Controllo personalizzato consiste nella possibilità di configurare i parametri in dettaglio. È possibile salvare le configurazioni come profili di controllo definiti dagli utenti che risultano particolarmente utili se il controllo viene eseguito più volte con gli stessi parametri.

Controllo supporti rimovibili

Simile alla funzione Controlla computer in uso, consente di avviare velocemente un controllo dei supporti rimovibili (come ad esempio CD/DVD/USB) attualmente collegati al computer. Questa opzione può rivelarsi utile in caso di connessione di una memoria USB a un computer e nel caso in cui si desideri ricercare malware e altre potenziali minacce.

Questo tipo di controllo può anche essere avviato facendo clic su **Controllo personalizzato**, selezionando **Supporti rimovibili** dal menu a discesa **Oggetti da controllare** e facendo clic su **Controllo**.

Ripeti ultimo controllo

Consente all'utente di avviare rapidamente il controllo eseguito in precedenza utilizzando le stessa impostazioni.

Per ulteriori informazioni sull'avanzamento del controllo, consultare il capitolo Avanzamento controllo.

NOTA: È consigliabile eseguire un controllo del computer almeno una volta al mese. Il controllo può essere configurato come attività pianificata in **Strumenti** > **Pianificazione attività**. Come pianificare un controllo del computer settimanale

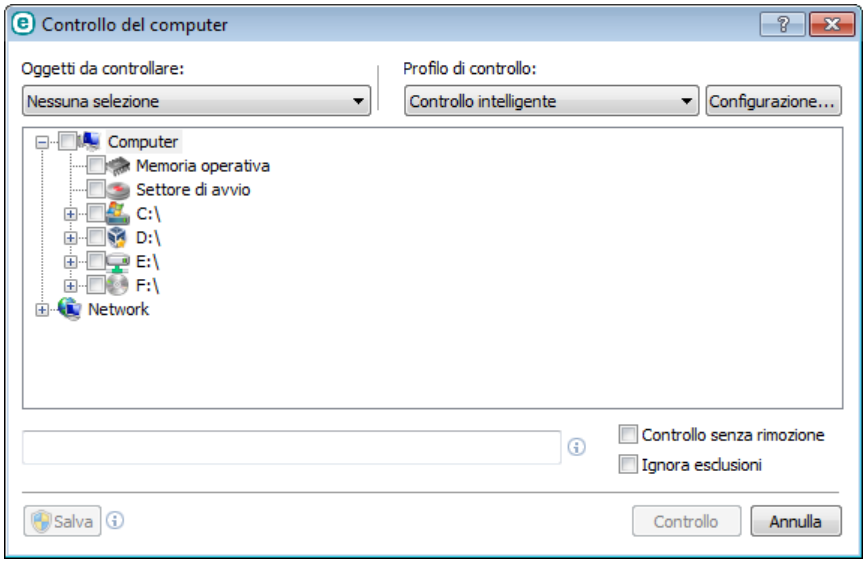
4.1.1.2.1 Launcher controllo personalizzato

Se non si desidera controllare l'intero spazio su disco ma solo una specifica destinazione, è possibile utilizzare lo strumento del Controllo personalizzato facendo clic su **Controllo computer** > **Controllo personalizzato** e selezionando un'opzione dal menu a discesa **Oggetti da controllare** oppure selezionando destinazioni specifiche dalla struttura (ad albero) della cartella.

La finestra Oggetti da controllare consente di definire gli oggetti (memoria, unità, settori, file e cartelle) che verranno sottoposti a controllo alla ricerca di infiltrazioni. Selezionare gli oggetti dalla struttura ad albero contenente un elenco di tutti i supporti disponibili nel computer. Il menu a discesa **Oggetti da controllare** consente di selezionare gli oggetti da controllare predefiniti.

- **Attraverso le impostazioni di profilo** - Consente di selezionare le destinazioni nel profilo di controllo selezionato.
- **Supporti rimovibili** - Consente di selezionare dischetti, supporti di archiviazione USB, CD/DVD.
- **Unità locali** - Consente di selezionare tutti gli hard disk del sistema.
- **Unità di rete** - Consente di selezionare tutte le unità di rete mappate.
- **Nessuna selezione** - Consente di annullare tutte le selezioni.

Per visualizzare rapidamente una destinazione di controllo o per aggiungere direttamente una destinazione desiderata (cartella o file), inserirla nel campo vuoto sotto all'elenco delle cartelle. Ciò è possibile solo se nella struttura ad albero non sono state selezionate destinazioni e il menu **Oggetti da controllare** è impostato su **Nessuna selezione**.



Gli elementi infetti non vengono puliti automaticamente. Il controllo senza rimozione può essere utilizzato per ottenere una panoramica dello stato di protezione corrente. Se si desidera effettuare solo un controllo del sistema senza azioni di pulizia aggiuntive, selezionare **Controlla senza pulire**. È inoltre possibile scegliere tra tre livelli di pulizia facendo clic su **Configurazione...** > **Pulizia**. Le informazioni relative alla scansione vengono salvate in un rapporto di scansione.

Se l'opzione **Ignora esclusioni** è selezionata, i file con estensioni precedentemente escluse dal controllo verranno sottoposti al controllo senza alcuna eccezione.

È possibile scegliere un profilo dal menu a discesa **Profilo di controllo** da utilizzare per il controllo delle destinazioni scelte. Il profilo predefinito è **Controlla il computer in uso**. Esistono due altri profili predefiniti chiamati **Controllo approfondito** e **Controllo menu contestuale**. Questi profili di controllo utilizzano diversi parametri ThreatSense. Fare clic su **Configurazione...** per configurare i dettagli del profilo di controllo scelto nel menu Profilo di controllo. Le opzioni disponibili sono descritte nella sezione **Altro** in Parametri ThreatSense.

Fare clic su **Salva** per salvare le modifiche apportate alle selezioni di destinazioni, comprese quelle relative alla struttura delle cartelle.

Fare clic su **Controlla** per eseguire il controllo utilizzando i parametri personalizzati configurati dall'utente.

Effettua controllo come Amministratore consente di eseguire il controllo mediante l'account Amministratore.

Selezionare questa opzione se l'utente corrente non dispone dei privilegi per accedere ai file appropriati da controllare. Nota: questo pulsante non è disponibile se l'utente corrente non può invocare operazioni UAC come Amministratore.

4.1.1.2.2 Avanzamento controllo

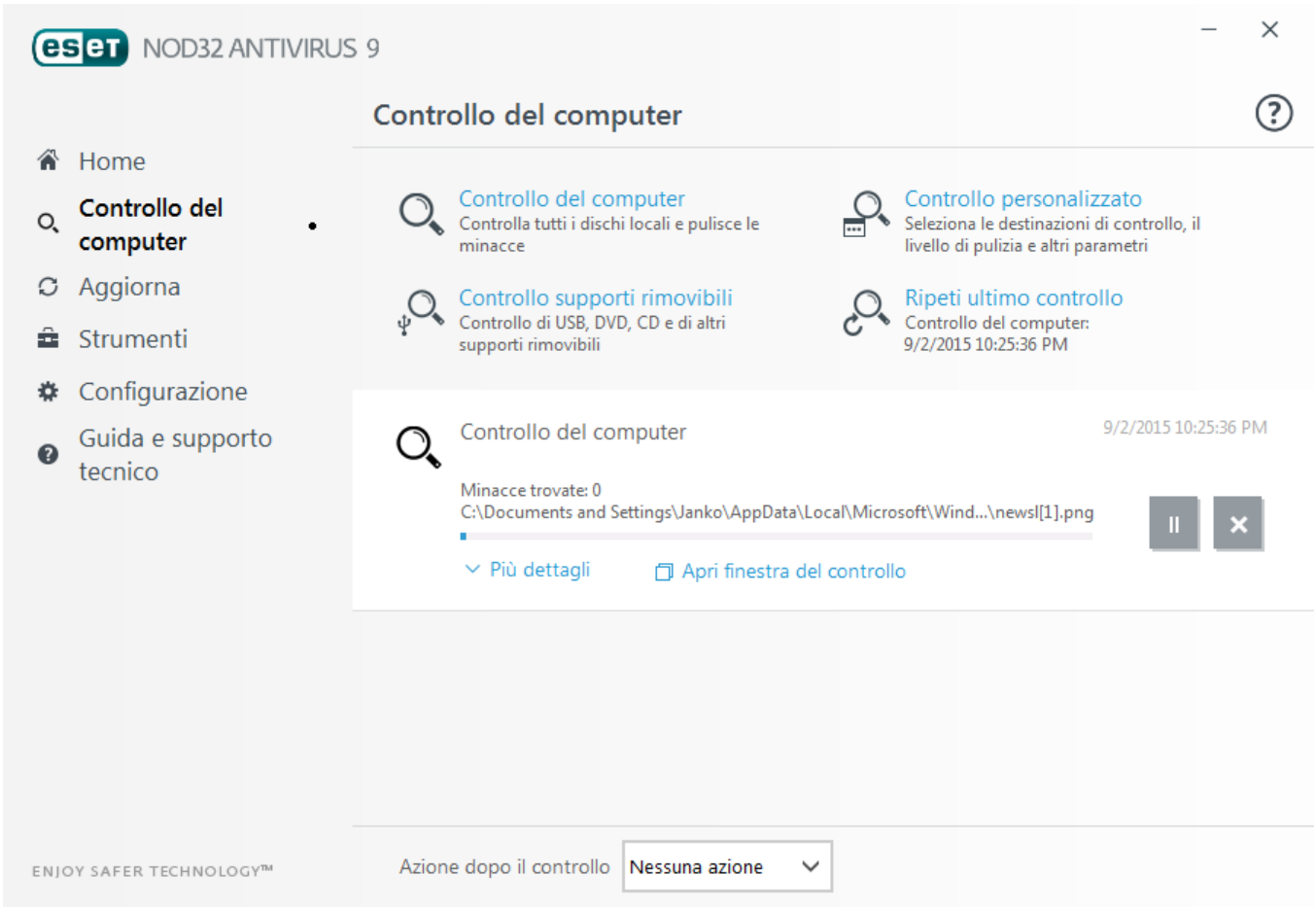
Nella finestra di avanzamento del controllo viene mostrato lo stato attuale del controllo e informazioni sul numero di file rilevati che contengono codice dannoso.

NOTA: è normale che alcuni file, ad esempio file protetti con password o file che vengono utilizzati esclusivamente dal sistema (in genere il file *pagefile.sys* e alcuni file di registro), non possano essere sottoposti al controllo.

Avanzamento controllo: la barra di avanzamento mostra lo stato di oggetti già sottoposti al controllo rispetto a quelli in attesa. Lo stato di avanzamento del controllo viene ricavato dal numero totale di oggetti inclusi nel controllo.
Destinazione: nome dell'oggetto in fase di controllo e relativo percorso.
Minacce trovate: mostra il numero totale di file sottoposti al controllo, minacce trovate e minacce pulite durante un controllo.
Sospendi: sospende un controllo.
Riprendi: questa opzione è visibile quando l'avanzamento del controllo è sospeso. Fare clic su **Riprendi** per continuare il controllo.
Interrompi: interrompe il controllo.
Scorri rapporto di controllo: se questa opzione è attiva, il rapporto di controllo scorrerà automaticamente quando vengono aggiunte nuove voci in modo da rendere visibili le voci più recenti.

SUGGERIMENTO:

Fare clic sulla lente di ingrandimento o sulla freccia per visualizzare i dettagli sul controllo attualmente in esecuzione.
È possibile eseguire un altro controllo parallelo facendo clic su **Controlla il computer in uso** o **Controllo personalizzato**.



Azione dopo il controllo: attiva un arresto o riavvio pianificato al termine del controllo del computer. Una volta terminato il controllo, verrà visualizzata una finestra di dialogo in cui viene richiesto all'utente di confermare l'arresto entro 60 secondi.

4.1.1.2.3 Profili di scansione

È possibile salvare i parametri di scansione preferiti per i controlli futuri. È consigliabile creare un profilo di scansione differente (con diversi oggetti da controllare, metodi di scansione e altri parametri) per ciascuna scansione utilizzata abitualmente.

Per creare un nuovo profilo, aprire la finestra Configurazione avanzata (F5) e fare clic su **Antivirus** > **Controllo computer su richiesta** > **Di base** > **Elenco di profili**. Nella finestra **Gestione profili** è disponibile un menu a discesa **Profili selezionati** contenente i profili di scansione esistenti e l'opzione per crearne di nuovi. Per ricevere assistenza durante la creazione di un profilo di controllo adatto alle proprie esigenze, consultare la sezione Configurazione parametri motore ThreatSense contenente una descrizione di ciascun parametro di configurazione del controllo.

Esempio: si supponga di voler creare il proprio profilo di controllo e che la configurazione **Controlla il computer in uso** sia appropriata solo in parte, in quanto non si desidera eseguire il controllo di eseguibili compressi o di applicazioni potenzialmente pericolose e si intende applicare l'opzione **Massima pulizia**. Inserire il nome del nuovo profilo nella finestra **Gestione profili** e fare clic su **Aggiungi**. Selezionare il nuovo profilo dal menu a discesa **Profilo selezionato**, modificare i parametri rimanenti in base alle proprie esigenze e fare clic su **OK** per salvare il nuovo profilo.

4.1.1.3 Controllo all'avvio

Per impostazione predefinita, all'avvio del sistema e durante gli aggiornamenti del database delle firme antivirali, verrà eseguito il controllo automatico del file di avvio. Questo controllo dipende dalla configurazione di Pianificazione configurazione e attività.

Le opzioni di controllo all'avvio fanno parte della pianificazione dell'attività **Controllo del file di avvio del sistema**. Per modificarne le impostazioni, accedere a **Strumenti** > **Pianificazione attività**, fare clic su **Verifica automaticamente file di avvio**, quindi su **Modifica**. Nell'ultimo passaggio verrà visualizzata la finestra Controllo automatico file di avvio (per ulteriori informazioni, vedere il capitolo seguente).

Per ulteriori informazioni sulla creazione e sulla gestione di Pianificazione attività, vedere Creazione di nuove attività.

4.1.1.3.1 Controllo automatico file di avvio

Durante la creazione di un'attività pianificata di controllo del file di avvio del sistema, sono disponibili varie opzioni per regolare i parametri seguenti:

Il menu a discesa **File utilizzati comunemente** specifica il livello di controllo dei file eseguiti all'avvio del sistema in base a un sofisticato algoritmo segreto. I file sono visualizzati in ordine decrescente in base ai seguenti criteri:

- **Tutti i file registrati** (la maggior parte dei file sottoposti al controllo)
- **File utilizzati raramente**
- **File utilizzati comunemente**
- **File utilizzati di frequente**
- **Solo i file utilizzati più di frequente** (ultimi file sottoposti al controllo)

Sono inoltre inclusi due gruppi specifici:

- **File eseguiti prima dell'accesso utente** - Contiene file da posizioni a cui è possibile accedere senza che l'utente abbia eseguito la registrazione (include quasi tutte le posizioni di avvio quali servizi, oggetti browser helper, notifiche Winlogon, voci della pianificazione attività di Windows, dll noti e così via).
- **File eseguiti dopo l'accesso utente** - Contiene file da posizioni a cui è possibile accedere solo dopo che un utente ha eseguito la registrazione (include file che sono eseguiti solo per un utente specifico, in genere i file in *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Per ogni gruppo summenzionato, vengono definiti elenchi di file da sottoporre al controllo.

Priorità di controllo - Il livello di priorità utilizzato per determinare il momento di avvio di un controllo:

- **Se in stato di inattività**: l'attività verrà eseguita solo quando il sistema è inattivo,
- **Più basso** (quando il carico di sistema è il più basso possibile),
- **Basso** (con un carico di sistema basso),
- **Normale** (con un carico di sistema medio).

4.1.1.4 Controllo stato inattivo

È possibile attivare lo scanner dello stato di inattività in **Configurazione avanzata** sotto ad **Antivirus** > **Controllo stato di inattività** > **Di base**. Impostare il pulsante accanto a **Attiva controllo stato inattivo** su **On** per attivare questa funzionalità. Se il computer si trova nello stato inattivo, verrà eseguito un controllo del computer silenzioso su tutti i dischi locali. Consultare la sezione Metodi di attivazione del rilevamento stato inattivo per un elenco completo di condizioni che è necessario soddisfare per attivare lo scanner dello stato inattivo.

Per impostazione predefinita, lo scanner dello stato inattivo non verrà eseguito in caso di alimentazione del computer (notebook) a batteria. È possibile ignorare questa impostazione attivando il pulsante accanto a **Esegui anche se il computer è alimentato a batteria** in Configurazione avanzata.

Attivare il pulsante **Attiva registrazione** in **Configurazione avanzata** > **Strumenti** > **ESET LiveGrid®** per registrare il risultato di un controllo del computer nella sezione File di rapporto (nella finestra principale del programma, fare clic su **Strumenti** > **File di rapporto** e selezionare **Controllo del computer** dal menu a discesa **Rapporto**.

Il rilevamento dello stato di inattività verrà eseguito se il computer si trova nei seguenti stati:

- Screen saver
- Blocco computer
- Uscita utente

Fare clic su Configurazione parametri motore ThreatSense per modificare i parametri di controllo (ad esempio, metodi di rilevamento) per lo scanner dello stato inattivo.

4.1.1.5 Esclusioni

Le esclusioni consentono di escludere file e cartelle dalla scansione. Per garantire che la ricerca delle minacce venga eseguita su tutti gli oggetti, si consiglia di creare esclusioni solo se assolutamente necessario. Tuttavia, esistono situazioni in cui potrebbe essere necessario escludere un oggetto, ad esempio il caso di voci di database di grandi dimensioni che rallenterebbero il computer durante il controllo o di un software che entra in conflitto con il controllo.

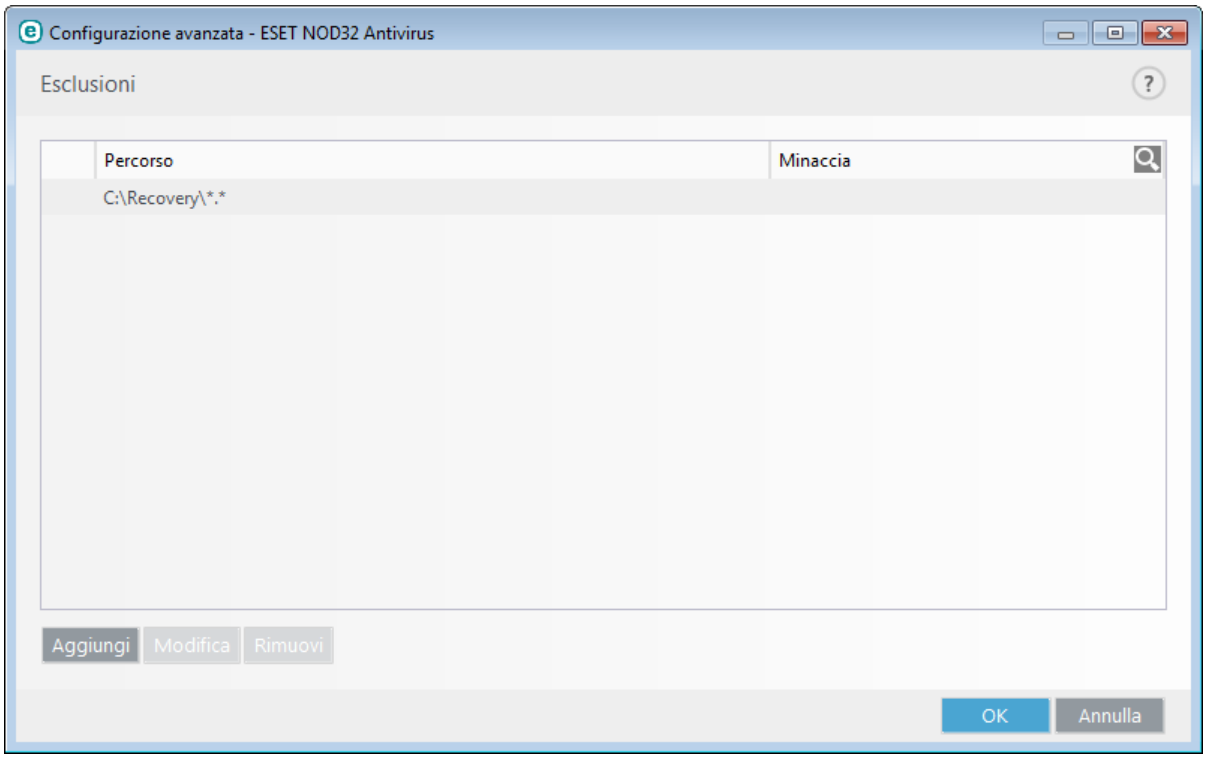
Per escludere un oggetto dalla scansione:

1. Fare clic su **Aggiungi**,
2. Immettere il percorso di un oggetto oppure selezionarlo nella struttura ad albero.

È possibile utilizzare i caratteri jolly per includere un gruppo di file. Un punto interrogativo (?) rappresenta un carattere variabile singolo, mentre un asterisco (*) rappresenta una stringa variabile di zero o più caratteri.

Esempi

- Se si desidera escludere tutti i file presenti in una cartella, digitare il percorso della cartella e utilizzare la maschera "*.*".
- Per escludere un'unità intera, compresi tutti i file e le sottocartelle, usare la maschera "D:*".
- Se si desidera escludere solo i file DOC, utilizzare la maschera "*.doc".
- Se il nome di un file eseguibile contiene un determinato numero di caratteri (e i caratteri variano) e si è sicuri solo della prima lettera (ad esempio "D"), utilizzare il formato seguente: "D????.exe". I punti interrogativi sostituiscono i caratteri mancanti (sconosciuti).



NOTA: una minaccia all'interno di un file non sarà rilevata dal modulo di protezione file system in tempo reale o dal modulo del controllo del computer se un file soddisfa i criteri dell'esclusione dal controllo.

Colonne

Percorso - Percorso dei file e delle cartelle esclusi.

Minaccia - Se è presente il nome di una minaccia accanto a un file escluso, significa che il file viene escluso solo per la minaccia indicata e non per tutte. Se il file si infetta successivamente con altri malware, verrà rilevato dal modulo antivirus. Questo tipo di esclusione può essere utilizzato solo per alcuni tipi di infiltrazioni e può essere creato nella finestra di avviso minaccia che segnala l'infiltrazione (fare clic su **Mostra opzioni avanzate**, quindi selezionare **Escludi dal rilevamento**), oppure fare clic su **Strumenti** > **Quarantena**, quindi fare clic con il pulsante destro del mouse sul file in quarantena e selezionare **Ripristina ed escludi dal rilevamento** dal menu contestuale.

Elementi di controllo

Aggiungi: esclude gli oggetti dal rilevamento.

Modifica: consente all'utente di modificare le voci selezionate.

Rimuovi: rimuove le voci selezionate.

4.1.1.6 Parametri di ThreatSense

ThreatSense è una tecnologia che prevede numerosi metodi di rilevamento di minacce complesse. Questa tecnologia è proattiva, ovvero fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. Il programma utilizza una combinazione di analisi del codice, emulazione del codice, firme generiche e firme antivirali che operano in modo integrato per potenziare enormemente la protezione del sistema. Il motore di controllo è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la percentuale di rilevamento. La tecnologia ThreatSense è inoltre in grado di eliminare i rootkit.

Le opzioni di configurazione del motore ThreatSense consentono all'utente di specificare vari parametri di controllo:

- Tipi ed estensioni dei file da controllare,
- Combinazione di diversi metodi di rilevamento,
- Livelli di pulizia e così via.

Per aprire la finestra di configurazione, fare clic su **Parametri di ThreatSense** nella finestra Configurazione avanzata di qualsiasi modulo che utilizza la tecnologia ThreatSense (vedere sezione sottostante). Scenari di protezione diversi potrebbero richiedere configurazioni diverse. Partendo da questo presupposto, ThreatSense è configurabile singolarmente per i seguenti moduli di protezione:

- Protezione file system in tempo reale,
- Controllo stato di inattività,
- Controllo all'avvio,
- Protezione documenti,
- Protezione client di posta,
- Protezione accesso Web,
- Controllo del computer.

I parametri di ThreatSense vengono ottimizzati per ciascun modulo e la relativa modifica può influire in modo significativo sul funzionamento del sistema. Ad esempio, la modifica dei parametri per il controllo degli eseguibili compressi o per consentire l'euristica avanzata nel modulo della protezione file system in tempo reale potrebbe causare un rallentamento del sistema (questi metodi di controllo vengono applicati generalmente solo ai file di nuova creazione). È quindi consigliabile non modificare i parametri predefiniti di ThreatSense per tutti i moduli, ad eccezione di Controllo del computer.

Oggetti da controllare

Questa sezione consente all'utente di definire i componenti e i file del computer nei quali verranno ricercate le infiltrazioni.

Memoria operativa: ricerca le minacce che attaccano la memoria operativa del sistema.

Settori di avvio: controlla i settori di avvio alla ricerca di virus nel record di avvio principale.

File di e-mail: il programma supporta le seguenti estensioni: DBX (Outlook Express) ed EML.

Archivi: il programma supporta le seguenti estensioni: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE e molte altri ancora.

Archivi autoestraenti: gli archivi autoestraenti (SFX) sono archivi che non necessitano di programmi speciali, ovvero archivi, per decomprimersi.

Eseguibili compressi: dopo essere stati eseguiti, gli eseguibili compressi (diversamente dai tipi di archivio standard) si decomprimono nella memoria. Oltre agli eseguibili compressi statici standard (UPS, yoda, ASPack, FSG e così via), lo scanner è in grado di riconoscere numerosi altri tipi di programmi di compressione grazie all'utilizzo dell'emulazione del codice.

Opzioni di controllo

Selezionare i metodi utilizzati durante la ricerca di infiltrazioni nel sistema. Sono disponibili le seguenti opzioni:

Euristica: l'euristica è un algoritmo che analizza l'attività (dannosa) dei programmi. Il vantaggio principale offerto da questa tecnologia consiste nella capacità di identificare software dannosi precedentemente inesistenti o non conosciuti dal database delle firme antivirali precedente. Lo svantaggio è una probabilità (minima) di falsi allarmi.

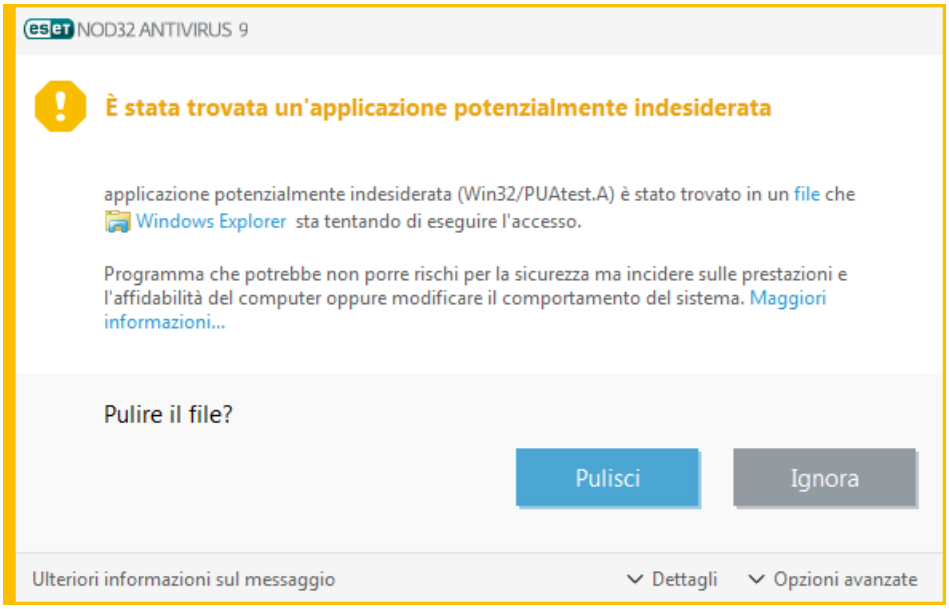
Euristica avanzata/DNA/Firme Smart: l'euristica avanzata si basa su un algoritmo di euristica esclusivo sviluppato da ESET, ottimizzato per il rilevamento dei worm e dei trojan horse e scritto in linguaggi di programmazione di alto livello. L'utilizzo dell'euristica avanzata determina un aumento esponenziale delle capacità di rilevamento delle minacce dei prodotti ESET. Le firme sono in grado di rilevare e identificare i virus in modo affidabile. Grazie al sistema di aggiornamento automatico, le nuove firme sono disponibili entro poche ore dal rilevamento di una minaccia. Lo svantaggio delle firme consiste nel fatto che tali strumenti rilevano solo i virus conosciuti (o versioni leggermente diverse di questi virus).

Un'applicazione potenzialmente indesiderata è un programma che contiene adware, installa barre degli strumenti o si prefigge altri obiettivi poco chiari. In alcuni casi, un utente potrebbe percepire che i vantaggi di un'applicazione potenzialmente indesiderata superano i rischi. Per questo motivo, ESET assegna a tali applicazioni una categoria a rischio ridotto rispetto ad altri tipi di software dannosi, come trojan horse o worm.

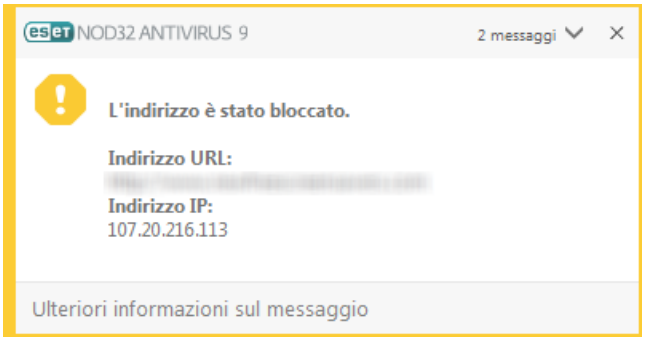
Avviso: trovata minaccia potenziale

In caso di rilevamento di un'applicazione potenzialmente indesiderata, l'utente potrà scegliere l'azione da intraprendere:

1. **Pulisci/Disconnetti**: questa opzione termina l'azione e impedisce alla minaccia potenziale di entrare nel sistema in uso.
2. **Ignora**: questa opzione consente a una minaccia potenziale di entrare nel sistema in uso.
3. Per consentire l'esecuzione futura dell'applicazione sul computer in uso senza interruzioni, fare clic su **Opzioni avanzate** e selezionare la casella di controllo accanto a **Escludi dal rilevamento**.

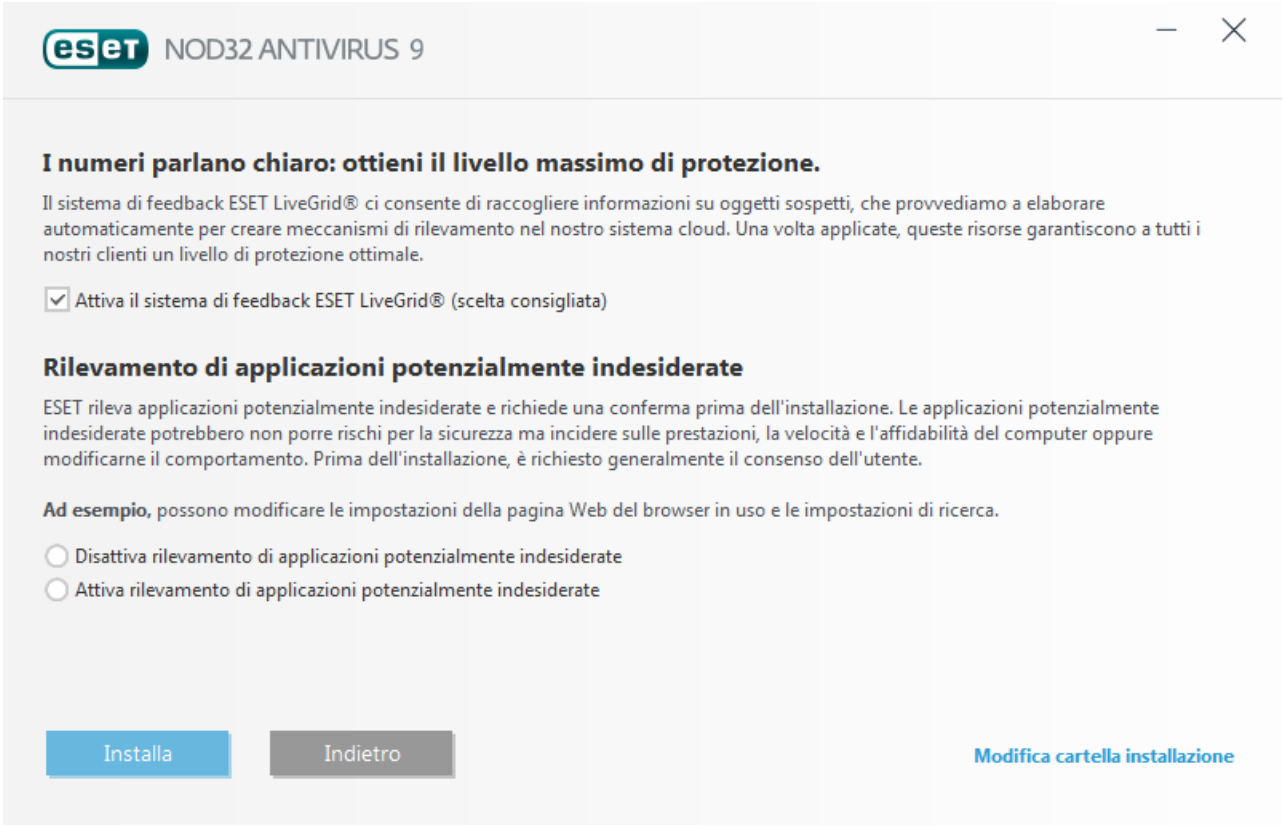

NOD32 ANTIVIRUS 9
È stata trovata un'applicazione potenzialmente indesiderata
applicazione potenzialmente indesiderata (Win32/PUAtest.A) è stato trovato in un file che
Windows Explorer sta tentando di eseguire l'accesso.
Programma che potrebbe non porre rischi per la sicurezza ma incidere sulle prestazioni e l'affidabilità del computer oppure modificare il comportamento del sistema. Maggiori informazioni...
Pulire il file?
Pulisci
Ignora
Ulteriori informazioni sul messaggio
Dettagli
Opzioni avanzate

Se un'applicazione potenzialmente indesiderata viene rilevata e non può essere pulita, verrà visualizzata la finestra di notifica **L'indirizzo è stato bloccato** nell'angolo in basso a destra della schermata. Per ulteriori informazioni su questo evento, accedere a **Strumenti** > **File di rapporto** > **Siti Web filtrati** dal menu principale.



Applicazioni potenzialmente indesiderate: impostazioni

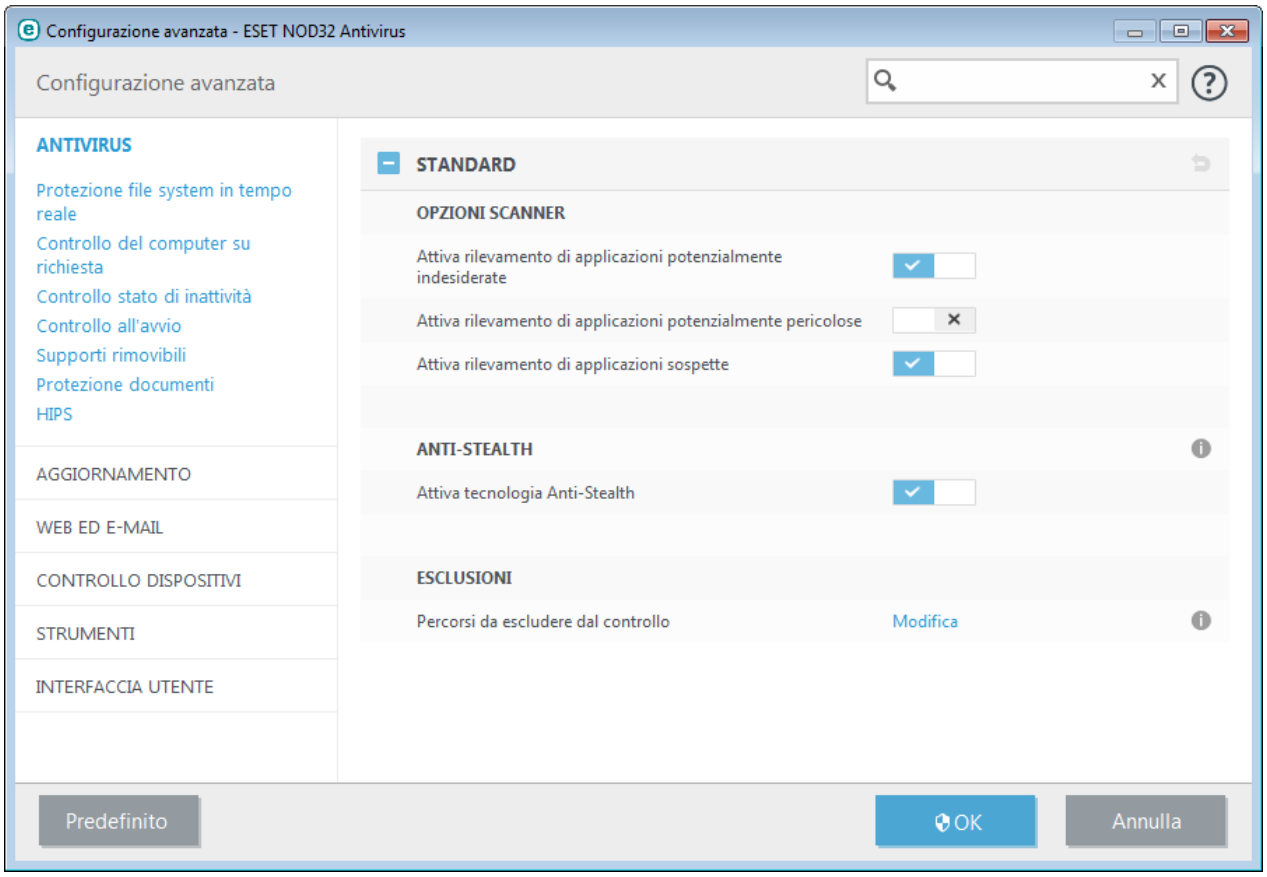
Durante l'installazione di un prodotto ESET, l'utente può decidere di attivare il rilevamento di applicazioni potenzialmente indesiderate, come illustrato di seguito:


NOD32 ANTIVIRUS 9
I numeri parlano chiaro: ottieni il livello massimo di protezione.
Il sistema di feedback ESET LiveGrid® ci consente di raccogliere informazioni su oggetti sospetti, che provvediamo a elaborare automaticamente per creare meccanismi di rilevamento nel nostro sistema cloud. Una volta applicate, queste risorse garantiscono a tutti i nostri clienti un livello di protezione ottimale.
Attiva il sistema di feedback ESET LiveGrid® (scelta consigliata)
Rilevamento di applicazioni potenzialmente indesiderate
ESET rileva applicazioni potenzialmente indesiderate e richiede una conferma prima dell'installazione. Le applicazioni potenzialmente indesiderate potrebbero non porre rischi per la sicurezza ma incidere sulle prestazioni, la velocità e l'affidabilità del computer oppure modificarne il comportamento. Prima dell'installazione, è richiesto generalmente il consenso dell'utente.
Ad esempio, possono modificare le impostazioni della pagina Web del browser in uso e le impostazioni di ricerca.
Disattiva rilevamento di applicazioni potenzialmente indesiderate
Attiva rilevamento di applicazioni potenzialmente indesiderate
Installa
Indietro
Modifica cartella installazione

Le applicazioni potenzialmente indesiderate possono installare adware e barre degli strumenti o contenere altre funzioni di programma non sicure e indesiderate.

Queste impostazioni possono essere modificate in qualsiasi momento. Per attivare o disattivare il rilevamento di applicazioni potenzialmente indesiderate, pericolose o sospette, attenersi alle seguenti istruzioni:

1. Aprire il prodotto ESET. Come faccio ad aprire il mio prodotto ESET?
2. Premere il tasto **F5** per accedere alla **Configurazione avanzata**.
3. Fare clic su **Antivirus** e attivare o disattivare le opzioni **Attiva rilevamento di applicazioni potenzialmente indesiderate**, **Attiva rilevamento di applicazioni potenzialmente pericolose** e **Attiva rilevamento di applicazioni sospette** in base alle proprie preferenze. Confermare facendo clic su **OK**.



Applicazioni potenzialmente indesiderate: wrapper di software

Il wrapper di un software è un tipo speciale di modifica di un'applicazione utilizzato da alcuni siti Web che offrono servizi di file hosting. Si tratta di uno strumento di terze parti che installa il programma che si intende scaricare aggiungendo, però, altri software, come ad esempio barre degli strumenti o adware. I software aggiuntivi possono inoltre apportare modifiche alla pagina iniziale del browser Web in uso e alle impostazioni di ricerca. Inoltre, i siti Web che offrono servizi di file hosting non comunicano al fornitore del software o al destinatario del download le modifiche apportate e non consentono di rifiutarle facilmente. Per tali motivi, ESET classifica i wrapper di software tra le applicazioni potenzialmente indesiderate per consentire agli utenti di decidere se accettare o meno il download.

Per una versione aggiornata di questa pagina della Guida, consultare questo articolo della Knowledge Base ESET.

Applicazioni potenzialmente pericolose: applicazioni potenzialmente pericolose è la classificazione utilizzata per programmi commerciali e legittimi, quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano le battute digitate da un utente). Questa opzione è disattivata per impostazione predefinita.

Le impostazioni di pulizia determinano il comportamento dello scanner durante la pulizia di file infetti. Sono disponibili 3 livelli di pulizia.

Esclusioni

Un'estensione è la parte del nome di un file delimitata da un punto. Un'estensione definisce il tipo e il contenuto di un file. Questa sezione della configurazione dei parametri di ThreatSense consente di definire i tipi di file da sottoporre a controllo.

Altro

Quando si configurano i parametri del motore ThreatSense per l'esecuzione di un Controllo computer su richiesta, nella sezione **Altro** sono disponibili anche le seguenti opzioni:

Flussi di dati alternativi (ADS): i flussi di dati alternativi utilizzati dal file system NTFS sono associazioni di file e cartelle invisibili alle normali tecniche di controllo. Molte infiltrazioni tentano di eludere il rilevamento camuffandosi in flussi di dati alternativi.

Esegui controlli in background con priorità bassa: ogni sequenza di controllo utilizza una determinata quantità di risorse del sistema. Se si utilizzano programmi che necessitano di molte risorse di sistema, è possibile attivare il controllo in background con priorità bassa e risparmiare risorse per le applicazioni.

Registra tutti gli oggetti: se questa opzione è selezionata, il file di rapporto riporta tutti i file sottoposti a controllo, anche quelli non infetti. Se ad esempio viene individuata un'infiltrazione all'interno di un archivio, nel rapporto verranno elencati anche i file puliti presenti all'interno dell'archivio.

Attiva ottimizzazione intelligente: al fine di garantire un livello di controllo ottimale, l'attivazione dell'ottimizzazione intelligente consente l'utilizzo delle impostazioni più efficienti mantenendo nel contempo la velocità di controllo più elevata. I vari moduli di protezione eseguono il controllo in modo intelligente, utilizzando metodi di controllo differenti e applicandoli a tipi di file specifici. Se l'opzione di ottimizzazione intelligente non è attivata, durante il controllo verranno applicate solo le impostazioni definite dall'utente nell'architettura ThreatSense dei moduli specifici.

Mantieni indicatore data e ora dell'ultimo accesso: selezionare questa opzione per mantenere l'ora di accesso originale ai file controllati anziché aggiornarli (ad esempio, per l'utilizzo con sistemi di backup di dati).

Limiti

La sezione Limiti consente all'utente di specificare la dimensione massima degli oggetti e i livelli di nidificazione degli archivi sui quali eseguire il controllo:

Impostazioni oggetti

Dimensione massima oggetto: definisce la dimensione massima degli oggetti su cui eseguire il controllo. Il modulo antivirus specifico eseguirà unicamente il controllo degli oggetti di dimensioni inferiori rispetto a quelle specificate. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di maggiori dimensioni dal controllo. Il valore predefinito è: *illimitato*.

Durata massima controllo dell'oggetto (sec.): definisce il valore temporale massimo per il controllo di un oggetto. Se è stato immesso un valore definito dall'utente, il modulo antivirus interromperà il controllo dell'oggetto una volta raggiunto tale valore, indipendentemente dal fatto che il controllo sia stato completato. Il valore predefinito è: *illimitato*.

Configurazione controllo degli archivi

Livello di nidificazione degli archivi: specifica il livello massimo di controllo degli archivi. Il valore predefinito è: *10*.

Dimensione massima file in archivio: questa opzione consente all'utente di specificare le dimensioni massime dei file contenuti all'interno degli archivi, i quali, una volta estratti, saranno sottoposti a controllo. Il valore predefinito è: *illimitato*.

NOTA: si consiglia di non modificare i valori predefiniti. In circostanze normali, non vi sono motivi particolari per eseguire tale operazione.

4.1.1.6.1 Pulizia

Le impostazioni di pulizia determinano il comportamento dello scanner durante la pulizia di file infetti. Sono disponibili 3 livelli di pulizia.

4.1.1.6.2 Estensioni file esclusi dal controllo

Un'estensione è una parte del nome di un file delimitata da un punto. Un'estensione definisce il tipo e il contenuto di un file. Questa sezione delle impostazioni parametri ThreatSense consente di definire i tipi di file da sottoporre a controllo.

Per impostazione predefinita, tutti i file vengono sottoposti a scansione indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dalla scansione.

L'esclusione di file è un'operazione utile nel caso in cui il controllo di determinati tipi di file impedisca il corretto funzionamento di uno specifico programma che utilizza determinate estensioni. Ad esempio, potrebbe essere consigliabile escludere le estensioni EDB, EML e TMP durante l'utilizzo dei server Microsoft Exchange.

I pulsanti **Aggiungi** e **Rimuovi** consentono all'utente di attivare o impedire il controllo di estensioni di file specifiche. Per aggiungere una nuova estensione all'elenco, fare clic su **Aggiungi**, digitare l'estensione nel campo vuoto e fare clic su **OK**. Dopo aver selezionato **Inserisci valori multipli**, è possibile aggiungere estensioni di file multiple delimitate da righe, virgole o punti e virgola. Attivando selezioni multiple, sarà possibile visualizzare le estensioni nell'elenco. Per eliminare un'estensione dall'elenco, selezionarla e fare clic su **Rimuovi**. Se si desidera modificare un'estensione selezionata, fare clic su **Modifica**.

È possibile utilizzare i simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco rappresenta qualsiasi stringa di caratteri, mentre il punto interrogativo rappresenta qualsiasi simbolo.

4.1.1.7 Rilevamento di un'infiltrazione

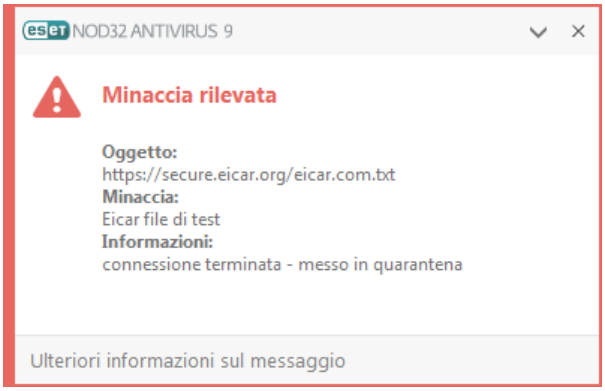
Le infiltrazioni possono raggiungere il sistema da diversi accessi, ad esempio pagine Web, cartelle condivise, messaggi e-mail o dispositivi rimovibili (USB, dischi esterni, CD, DVD, dischetti e così via).

Comportamento standard

In linea generale, ESET NOD32 Antivirus gestisce le infiltrazioni utilizzando i seguenti strumenti per la rilevazione:

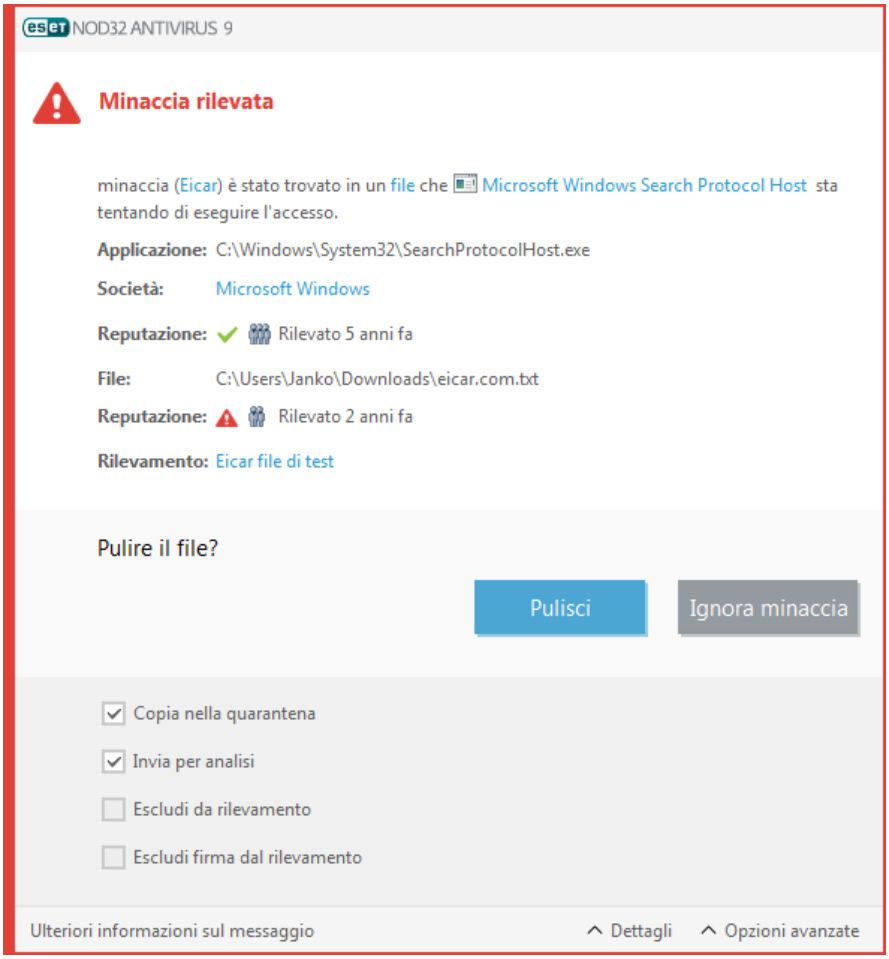
- Protezione file system in tempo reale
- Protezione accesso Web
- Protezione client di posta
- Controllo del computer su richiesta

Ciascuna di tali opzioni utilizza il livello di pulizia standard e tenta di pulire il file e di spostarlo nella Quarantena o di interrompere la connessione. Una finestra di avviso viene visualizzata nell'area di notifica posta nell'angolo in basso a destra della schermata. Per ulteriori informazioni sui livelli di pulizia e sul comportamento, consultare il paragrafo Pulizia.



Pulizia ed eliminazione

In assenza di azioni predefinite per l'esecuzione della Protezione file system in tempo reale, verrà chiesto all'utente di selezionare un'opzione nella finestra di avviso. Le opzioni generalmente disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, in quanto i file infettati non verranno puliti. È opportuno selezionare questa opzione solo quando si è certi che un file non è pericoloso e che si tratta di un errore di rilevamento.



Applicare la pulizia nel caso in cui un file sia stato attaccato da un virus che ha aggiunto un codice dannoso. In tal caso, tentare innanzitutto di pulire il file infetto per ripristinarne lo stato originale. Nel caso in cui il file sia composto esclusivamente da codice dannoso, verrà eliminato.

Se un file infetto è "bloccato" o utilizzato da un processo del sistema, verrà eliminato solo dopo essere stato rilasciato (generalmente dopo il riavvio del sistema).

Più minacce

Se durante un controllo del computer i file infetti non sono stati puliti (o se il Livello di pulizia era impostato su **Nessuna pulizia**), viene visualizzata una finestra di avviso che richiede di selezionare le azioni per i file in questione. Selezionare le azioni da eseguire sui file (le azioni vengono impostate singolarmente per ciascun file presente nell'elenco), quindi fare clic su **Fine**.

Eliminazione dei file negli archivi

In modalità di pulizia predefinita, l'intero archivio verrà eliminato solo nel caso in cui contenga file infetti e nessun file pulito. In pratica, gli archivi non vengono eliminati nel caso in cui dovessero contenere anche file puliti non dannosi. Durante l'esecuzione di un controllo di massima pulizia, si consiglia di agire con estrema prudenza, in quanto, in caso di rilevamento di un file infetto, verrà eliminato l'intero archivio di appartenenza dell'oggetto, indipendentemente dallo stato degli altri file.

Se il computer mostra segnali di infezione malware, ad esempio appare più lento, si blocca spesso e così via, è consigliabile attenersi alle seguenti istruzioni:

- Aprire ESET NOD32 Antivirus e fare clic su Controllo del computer
- Fare clic su **Controlla il computer in uso** (per ulteriori informazioni, consultare il paragrafo Controllo del computer)
- Al termine del controllo, consultare il rapporto per conoscere il numero di file controllati, infetti e puliti

Se si desidera controllare solo una parte del disco, fare clic su **Controllo personalizzato** e selezionare le destinazioni su cui effettuare un controllo antivirus.

4.1.1.8 Protezione documenti

La funzione Protezione documenti consente di eseguire il controllo dei documenti di Microsoft Office prima della loro apertura e dei file scaricati automaticamente da Internet Explorer, ad esempio gli elementi di Microsoft ActiveX. La funzione Protezione documenti offre un livello di protezione aggiuntivo rispetto alla protezione file system in tempo reale e può essere disattivata per ottimizzare le prestazioni di sistemi non esposti a volumi elevati di documenti Microsoft Office.

Integrazione nel sistema consente di attivare il sistema di protezione. Per modificare questa opzione, premere F5 per aprire la finestra Configurazione avanzata e fare clic su **Antivirus** > **Protezione documenti** nella finestra **Configurazione avanzata**.

Questa funzione è attivata dalle applicazioni che utilizzano Microsoft Antivirus API (ad esempio, Microsoft Office 2000 e versioni successive o Microsoft Internet Explorer 5.0 e versioni successive).

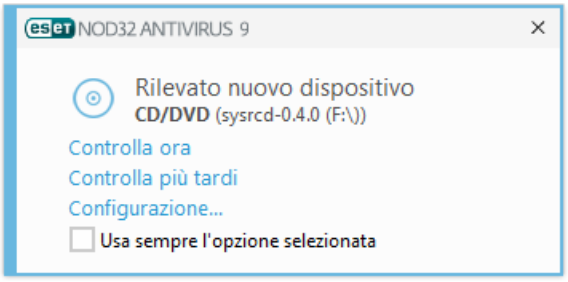
4.1.2 Supporti rimovibili

ESET NOD32 Antivirus offre il controllo automatico dei supporti rimovibili (CD/DVD/USB/...). Questo modulo consente di controllare un supporto inserito. Questa funzionalità può essere utile se l'amministratore del computer desidera impedire l'utilizzo di supporti rimovibili con contenuti non desiderati da parte degli utenti.

Azione da eseguire all'inserimento dei supporti rimovibili: selezionare l'azione predefinita che verrà eseguita quando un supporto rimovibile viene inserito nel computer (CD/DVD/USB). Selezionando **Mostra opzioni di controllo**, verrà visualizzata una notifica che consente all'utente di scegliere un'azione desiderata:

- **Non controllare**: non verrà eseguita alcuna azione e la finestra **Rilevato nuovo dispositivo** verrà chiusa.
- **Controllo automatico del dispositivo**: viene eseguito il controllo del computer su richiesta del supporto rimovibile inserito.
- **Mostra opzioni di controllo**: apre la sezione di configurazione dei supporti rimovibili.

All'inserimento di un supporto rimovibile, viene visualizzata la seguente finestra di dialogo:



Controlla ora: avvia il controllo del supporto rimovibile.

Controlla più tardi: il controllo del supporto rimovibile verrà posticipato.

Configurazione: apre la Configurazione avanzata.

Usa sempre l'opzione selezionata: se l'opzione è selezionata, verrà eseguita la stessa azione quando viene inserito nuovamente un supporto rimovibile.

In ESET NOD32 Antivirus è inoltre disponibile la funzionalità Controllo dispositivi che consente all'utente di definire

regole per l'utilizzo dei dispositivi esterni su un determinato computer. Per ulteriori informazioni sul Controllo dispositivi, consultare il paragrafo Controllo dispositivi.

4.1.3 Controllo dispositivi

ESET NOD32 Antivirus offre un controllo automatico dei dispositivi (CD/DVD/USB/...). Questo modulo consente di controllare, bloccare o regolare le estensioni dei filtri o delle autorizzazioni e di definire la capacità dell'utente di accedere e di utilizzare un determinato dispositivo. Questa funzionalità potrebbe rivelarsi utile nel caso in cui l'amministratore di un computer desideri impedire l'utilizzo di dispositivi con contenuti non desiderati da parte degli utenti.

Dispositivi esterni supportati:

- Archiviazione su disco (HDD, disco rimovibile USB)
- CD/DVD
- Stampante USB
- Archiviazione FireWire
- Dispositivo Bluetooth
- Lettore di smart card
- Dispositivo di acquisizione immagini
- Modem
- Porta LPT/COM
- Dispositivo portatile
- Tutti i tipi di dispositivi

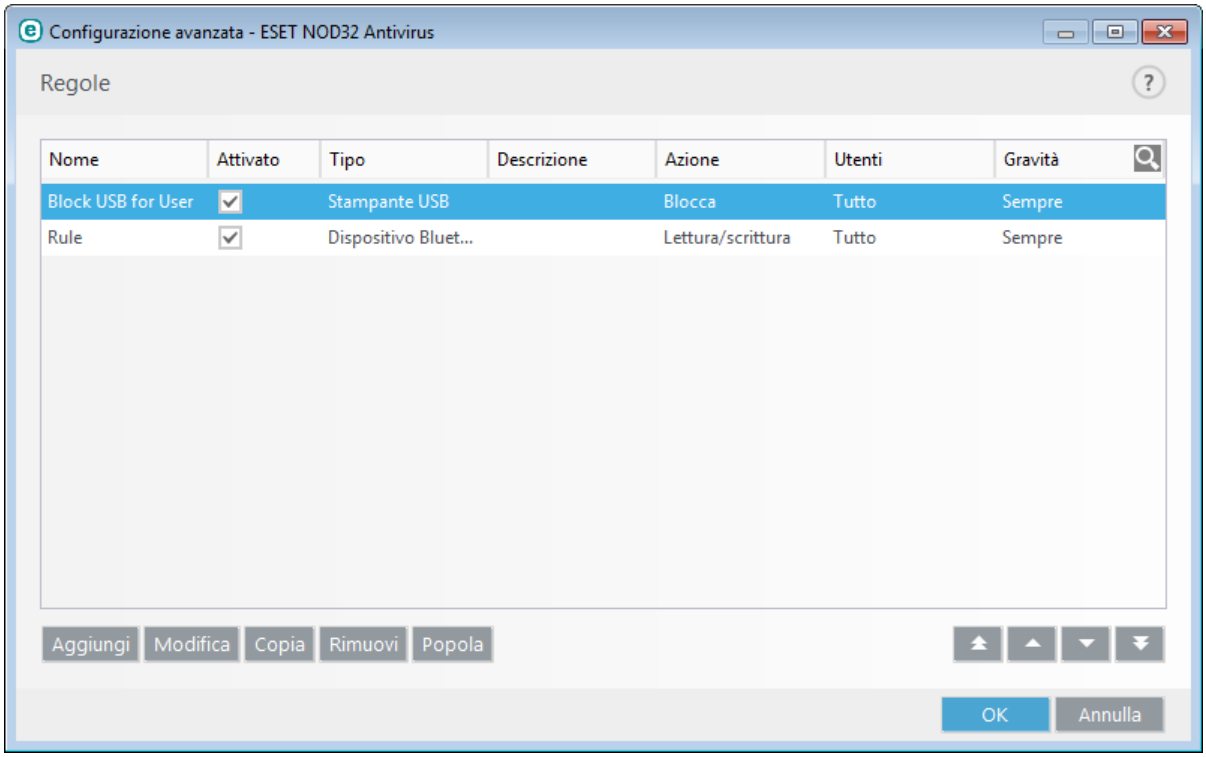
Le opzioni di configurazione del controllo dispositivi possono essere modificate in **Configurazione avanzata** (F5) > **Controllo dispositivi**.

Attivando il pulsante accanto a **Integra nel sistema**, è possibile attivare la funzione Controllo dispositivi in ESET NOD32 Antivirus. Per rendere effettiva questa modifica, sarà necessario riavviare il computer. Dopo aver attivato il Controllo dispositivi, si attiverà **Regole**, che consentirà all'utente di aprire la finestra Editor regole.

In caso di inserimento di un dispositivo bloccato mediante una regola esistente, verrà visualizzata una finestra di notifica e l'accesso al dispositivo non verrà concesso.

4.1.3.1 Editor regole controllo dispositivi

Nella finestra **Editor regole controllo dispositivi**, in cui vengono visualizzate le regole esistenti, è possibile effettuare un controllo accurato dei dispositivi esterni collegati dagli utenti al computer.



È possibile consentire o bloccare specifici dispositivi per ciascun utente o gruppo di utenti e sulla base di parametri aggiuntivi del dispositivo che è possibile specificare nella configurazione delle regole. L'elenco delle regole contiene varie descrizioni tra cui nome, tipo di dispositivo esterno, azione da eseguire dopo aver collegato un dispositivo esterno al computer e gravità del rapporto.

Fare clic su **Aggiungi** o **Modifica** per gestire una regola. Fare clic su **Copia** per creare una nuova regola con le opzioni predefinite utilizzate per un'altra regola selezionata. Le stringhe XML visualizzate quando si seleziona una regola possono essere copiate negli Appunti in modo da aiutare gli amministratori di sistema a esportare/importare questi dati e utilizzarli, ad esempio, in ESET Remote Administrator.

Premere CTRL e fare clic per selezionare più regole e applicare azioni, come ad esempio elimina o sposta in alto o in basso nell'elenco, a tutte le regole selezionate. La casella di controllo **Attivata** consente di disattivare o attivare una regola. Questa opzione è utile se non si desidera eliminare definitivamente una regola in modo da poterla utilizzare in futuro.

Il controllo viene eseguito mediante regole classificate in base al rispettivo ordine di priorità (le regole con priorità maggiore saranno posizionate in alto).

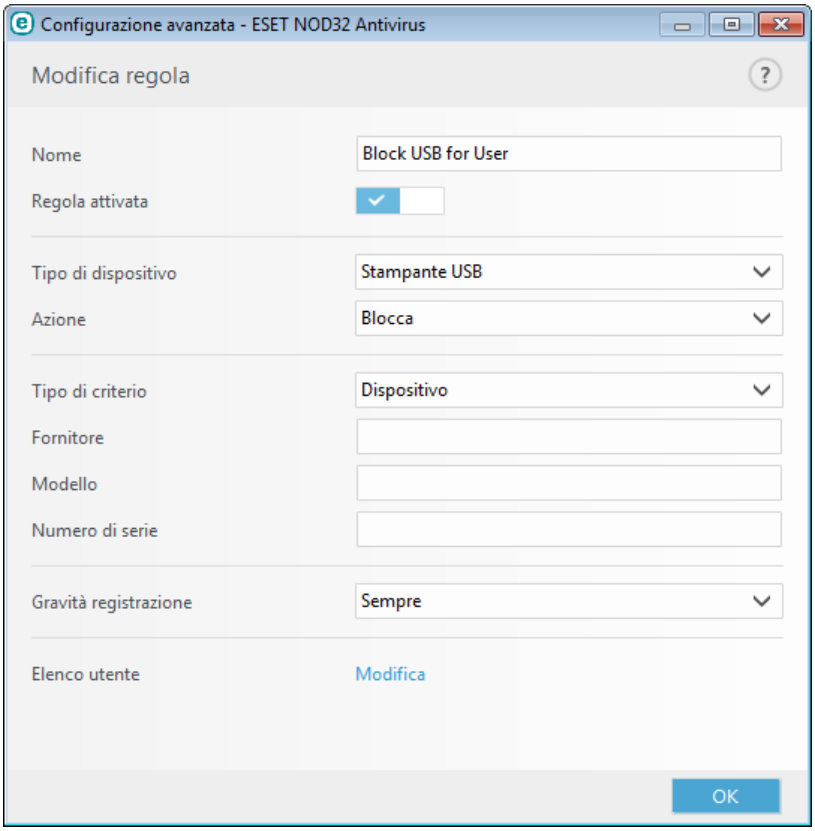
Le voci del rapporto possono essere visualizzate nella finestra principale di ESET NOD32 Antivirus in **Strumenti** > **File di rapporto**.

Il rapporto Controllo dispositivi registra tutte le occorrenze di attivazione del controllo dispositivi.

Fare clic su **Popola** per popolare automaticamente i parametri dei supporti rimovibili per i dispositivi collegati al computer.

4.1.3.2 Aggiunta di regole per il controllo dispositivi

Una regola per il controllo dispositivi definisce l'azione che verrà intrapresa quando viene effettuata una connessione tra il computer e un dispositivo che soddisfa i criteri della regola.



Inserire una descrizione della regola nel campo **Nome** per consentire una migliore identificazione. Fare clic sul pulsante accanto a **Regola attivata** per disattivare o attivare questa regola. Questa opzione può essere utile se non si desidera eliminare definitivamente la regola.

Tipo di dispositivo

Scegliere il tipo di dispositivo esterno dal menu a discesa (Archiviazione su disco/Dispositivo portatile/Bluetooth/FireWire/...). Le informazioni relative al tipo di dispositivo vengono raccolte dal sistema operativo e possono essere visualizzate in Gestione dispositivi del sistema se un dispositivo è collegato al computer. I supporti di archiviazione includono dischi esterni o lettori tradizionali di schede di memoria collegati tramite USB o FireWire. I lettori di smart card includono circuiti integrati incorporati, come ad esempio schede SIM o schede di autenticazione. Esempi di dispositivi di acquisizione immagini sono gli scanner o le fotocamere. Poiché tali dispositivi non forniscono informazioni sugli utenti, ma solo sulle azioni, possono essere bloccati solo a livello globale.

Azione

È possibile consentire o bloccare l'accesso ai dispositivi non adatti all'archiviazione. Le regole dei dispositivi di archiviazione consentono invece all'utente di scegliere uno dei seguenti diritti:

- **Lettura/scrittura** - Sarà consentito l'accesso completo al dispositivo.
- **Blocca**: l'accesso al supporto verrà bloccato.
- **Solo lettura**: sul dispositivo sarà consentito l'accesso di sola lettura.
- **Avvisa**: tutte le volte che un dispositivo effettua la connessione, all'utente verrà inviata una notifica che lo avvisa in merito all'eventuale autorizzazione/blocco e verrà creata una voce di rapporto. Poiché i dispositivi non vengono memorizzati, l'utente visualizzerà sempre una notifica relativa alle successive connessioni di uno stesso dispositivo.

Tenere presente che non sono disponibili tutte le azioni (autorizzazioni) per tutti i tipi di dispositivi. Se si tratta di un dispositivo di archiviazione, saranno disponibili tutte e quattro le azioni. Per i dispositivi non di archiviazione, sono disponibili solo tre azioni (ad esempio, l'azione **Solo lettura** non è disponibile per il sistema Bluetooth. Ciò

significa che i dispositivi Bluetooth possono essere solo consentiti, bloccati o avvisati).

Tipo di criterio : selezionare **Gruppo dispositivi** o **Dispositivo.**

I parametri aggiuntivi visualizzati di seguito possono essere utilizzati per ottimizzare le regole e personalizzarle in base ai dispositivi in uso. Tutti i parametri non fanno distinzione tra lettere maiuscole e minuscole:

- **Fornitore**: filtraggio in base al nome o all'identificativo del fornitore.
- **Modello** - Nome specifico del dispositivo.
- **Numero di serie**: generalmente, a ogni dispositivo esterno è associato un numero di serie. Nel caso di CD/DVD, il numero di serie è associato al supporto specifico e non all'unità CD.

NOTA: se i parametri non sono definiti, la regola ignorerà questi campi durante la ricerca delle corrispondenze. I parametri di filtraggio in tutti i campi di testo non fanno distinzione tra maiuscole e minuscole e i caratteri jolly (*, ?) non sono supportati.

SUGGERIMENTO: per visualizzare le informazioni relative a un dispositivo, creare una regola per tale dispositivo specifico, collegare il dispositivo al computer in uso e verificare i dettagli relativi al dispositivo nel Rapporto controllo dispositivi.

Gravità registrazione

ESET NOD32 Antivirus salva tutti gli eventi importanti in un file di rapporto, che può essere visualizzato direttamente dal menu principale. Fare clic su **Strumenti** > **File di rapporto**, quindi selezionare **Controllo dispositivo** dal menu a discesa **Rapporto**.

- **Sempre** : registra tutti gli eventi.
- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma.
- **Informazioni**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarme**: registra errori critici e messaggi di allarme.
- **Nessuno**: non verrà registrato alcun rapporto.

Le regole possono essere limitate a determinati utenti o gruppi di utenti aggiunti all'**Elenco utenti**:

- **Aggiungi**: apre la finestra di dialogo **Tipi di oggetto: Utenti o Gruppi**, che consente di selezionare gli utenti desiderati.
- **Rimuovi**: rimuove l'utente selezionato dal filtro.

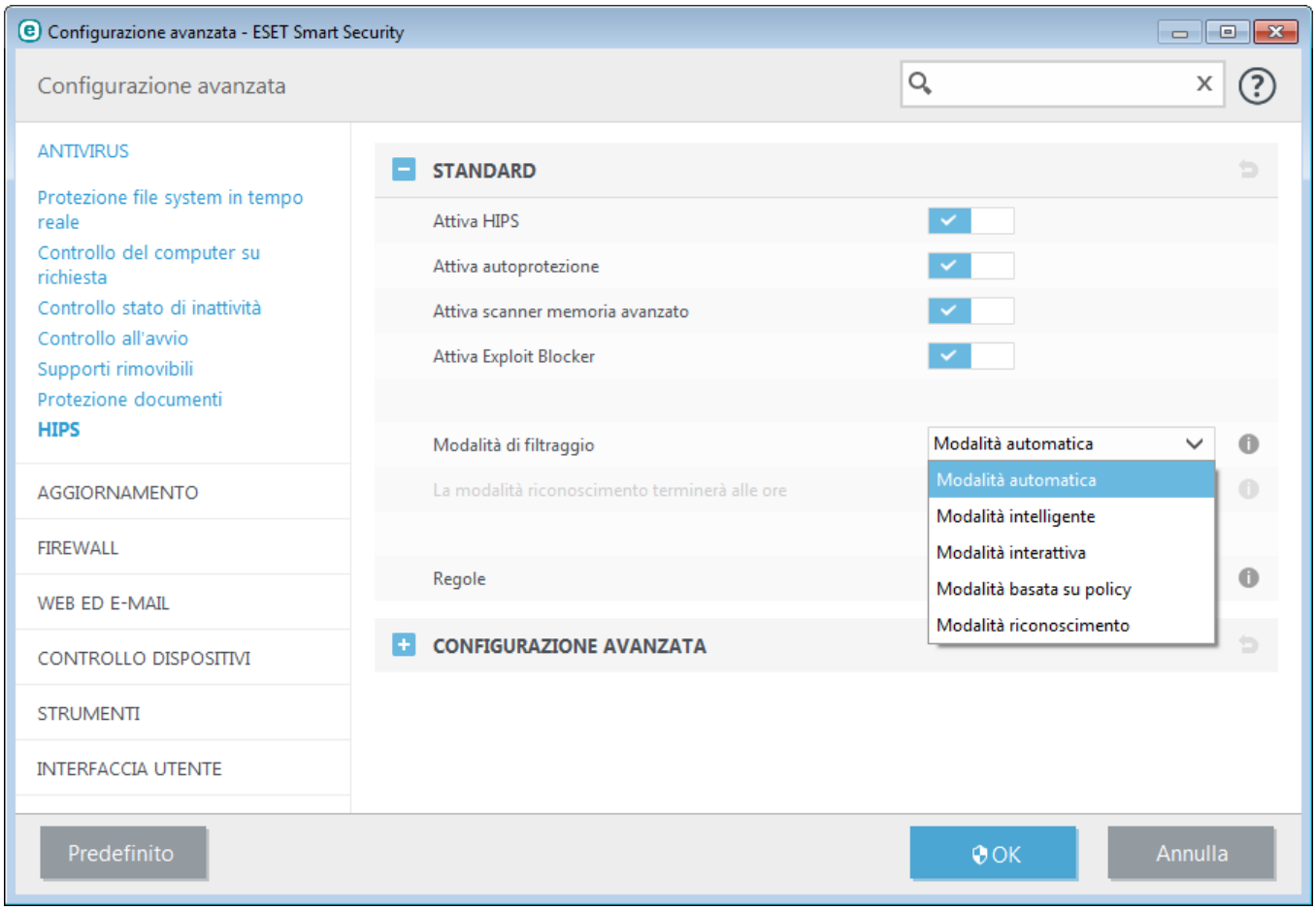
NOTA: tutti i dispositivi possono essere filtrati dalle regole dell'utente (ad esempio, i dispositivi di acquisizione di immagini non forniscono informazioni sugli utenti, ma solo sulle azioni).

4.1.4 Sistema anti-intrusione basato su host (HIPS)

È consigliabile che le modifiche delle impostazioni HIPS siano apportate solo dagli utenti avanzati. Una configurazione non corretta delle impostazioni HIPS può causare instabilità di sistema.

Il **Sistema anti-intrusione basato su host** (HIPS) protegge il sistema da malware e attività indesiderate che tentano di compromettere la sicurezza del computer. L'HIPS utilizza un'analisi comportamentale avanzata unita alle capacità di rilevamento del filtraggio di rete per il monitoraggio dei processi in esecuzione, dei file e delle chiavi del registro. L'HIPS è indipendente dalla protezione file system in tempo reale e non è un firewall, in quanto monitora solo i processi eseguiti all'interno del sistema operativo.

Le impostazioni HIPS sono disponibili in **Configurazione avanzata** (F5) > **Antivirus** > **HIPS** > **Di base**. Lo stato HIPS (attivato/disattivato) è visualizzato nella finestra principale del programma ESET NOD32 Antivirus in **Configurazione** > **Protezione computer**.



ESET NOD32 Antivirus utilizza una tecnologia di **Autoprotezione** integrata che impedisce a software dannosi di danneggiare o disattivare la protezione antivirus e antispyware, in modo da garantire costantemente la protezione del sistema. È necessario riavviare Windows per disattivare l'HIPS o l'Autoprotezione.

Lo **Scanner memoria avanzato** lavora congiuntamente all'Exploit Blocker per rafforzare il livello di protezione contro malware concepiti allo scopo di eludere il rilevamento dei prodotti antimalware mediante l'utilizzo di pratiche di offuscamento o crittografia. Per impostazione predefinita, lo scanner di memoria avanzato è attivato. Per ulteriori informazioni su questo tipo di protezione, consultare il glossario.

L'**Exploit Blocker** è progettato per rafforzare i tipi di applicazione comunemente utilizzati come browser Web, lettori PDF, client di posta e componenti di MS Office. L'exploit blocker è attivato per impostazione predefinita. Per ulteriori informazioni su questo tipo di protezione, consultare il glossario.

Il filtraggio può essere eseguito in una delle quattro seguenti modalità:

Modalità automatica: le operazioni sono attivate, ad eccezione di quelle bloccate dalle regole predefinite che proteggono il sistema.

Modalità intelligente: all'utente verranno segnalati solo gli eventi molto sospetti.

Modalità interattiva: all'utente verrà richiesto di confermare le operazioni.

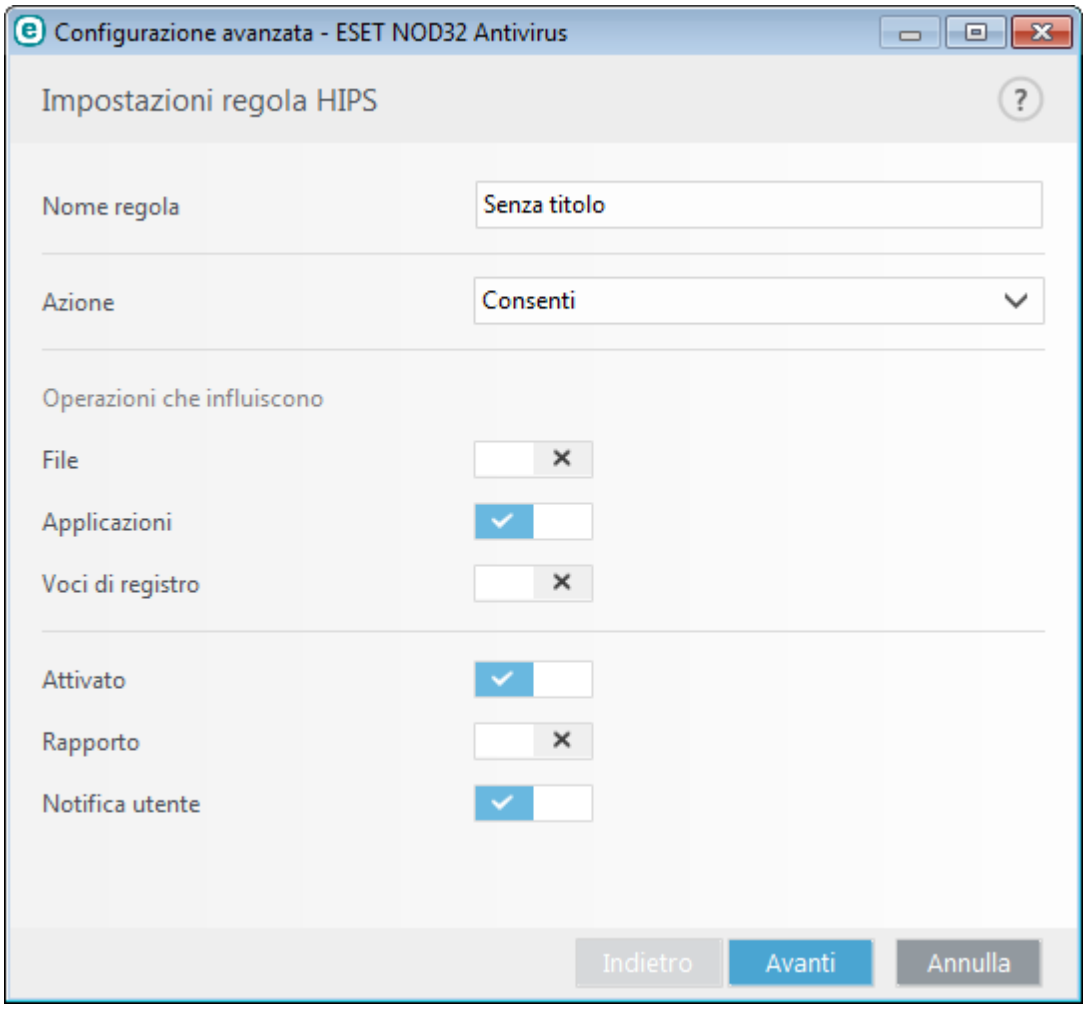
Modalità basata su criteri: le operazioni sono bloccate.

Modalità riconoscimento - Le operazioni sono attivate e dopo ogni operazione viene creata una regola. Le regole create in questa modalità possono essere visualizzate nell'Editor regole, ma la loro priorità è inferiore rispetto alla priorità delle regole create manualmente o delle regole create nella modalità automatica. Selezionando la Modalità riconoscimento dal menu a discesa Modalità filtraggio HIPS, sarà disponibile l'impostazione **La modalità riconoscimento terminerà alle ore**. Selezionare la durata per la quale si desidera attivare la modalità riconoscimento, tenendo presente che il limite massimo è di 14 giorni. Una volta trascorsa la durata specificata, all'utente verrà richiesto di modificare le regole create dall'HIPS quando si trovava in modalità riconoscimento. È inoltre possibile scegliere un'altra modalità di filtraggio oppure posticipare la decisione e continuare a utilizzare la modalità riconoscimento.

Il sistema HIPS monitora gli eventi all'interno del sistema operativo e reagisce in base a regole simili a quelle utilizzate dal rapporto del Personal firewall. Fare clic su **Modifica** per aprire la finestra di gestione delle regole HIPS. In questa sezione è possibile selezionare, creare, modificare o eliminare regole.

Nell'esempio seguente viene spiegato come limitare il comportamento indesiderato delle applicazioni:

1. Denominare la regola e selezionare **Blocca** nel menu a discesa **Azione**.
2. Attivare il pulsante **Notifica utente** per visualizzare una notifica tutte le volte che viene applicata una regola.
3. Selezionare almeno un'operazione alla quale verrà applicata la regola. Nella finestra **Applicazioni di origine**, selezionare**Tutte le applicazioni** dal menu a discesa per applicare la nuova regola a tutte le applicazioni che tentano di eseguire una delle operazioni dell'applicazione selezionata sulle applicazioni specificate dall'utente.
4. Selezionare **Modifica stato di un'altra applicazione** (tutte le operazioni sono descritte nella guida del prodotto, a cui è possibile accedere premendo F1).
5. Selezionare **Applicazioni specifiche** dal menu a discesa, quindi **Aggiungi** per aggiungere una o più applicazioni che si desidera proteggere.
6. Fare clic su **Fine** per salvare la nuova regola.



4.1.4.1 Configurazione avanzata

Le seguenti opzioni sono utili per eseguire il debug e l'analisi del comportamento di un'applicazione:

Caricamento driver sempre consentito: i driver selezionati sono sempre autorizzati a caricare indipendentemente dalla modalità di filtraggio configurata, eccetto nel caso in cui vengano bloccati esplicitamente da una regola dell'utente.

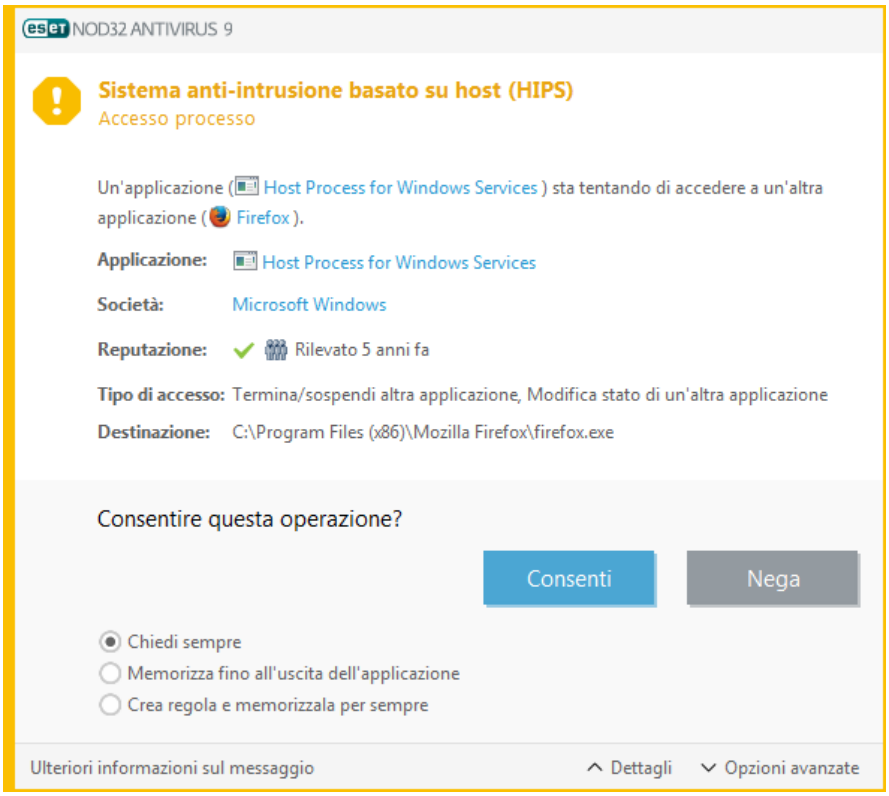
Registra tutte le operazioni bloccate - Tutte le operazioni bloccate verranno scritte sul registro HIPS.

Notifica quando si verificano modifiche nelle applicazioni all'Avvio - Consente di visualizzare una notifica sul desktop ogni volta che un'applicazione viene aggiunta o rimossa dall'avvio del sistema.

Per una versione aggiornata di questa pagina della Guida, consultare l'articolo della Knowledge Base ESET.

4.1.4.2 Finestra interattiva HIPS

Se l'azione predefinita di una regola è impostata su **Chiedi**, verrà visualizzata una finestra di dialogo tutte le volte che la regola verrà attivata. È possibile scegliere di **Negare** o **Consentire** l'operazione. Se l'utente non sceglie un'azione nell'intervallo di tempo specifico, verrà selezionata una nuova azione in base alle regole.


NOD32 ANTIVIRUS 9
Sistema anti-intrusione basato su host (HIPS)
Accesso processo
Un'applicazione (Host Process for Windows Services) sta tentando di accedere a un'altra applicazione (Firefox).
Applicazione: Host Process for Windows Services
Società: Microsoft Windows
Reputazione: Rilevato 5 anni fa
Tipo di accesso: Termina/sospendi altra applicazione, Modifica stato di un'altra applicazione
Destinazione: C:\Program Files (x86)\Mozilla Firefox\firefox.exe
Consentire questa operazione?
Consenti
Nega
Chiedi sempre
Memorizza fino all'uscita dell'applicazione
Crea regola e memorizzala per sempre
Ulteriori informazioni sul messaggio
Dettagli
Opzioni avanzate

La finestra di dialogo consente all'utente di creare una regola in base a una qualsiasi nuova azione rilevata dall'HIPS e di definire le condizioni in base alle quali consentire o negare l'azione. Per accedere ai parametri corretti, fare clic su **Dettagli**. Le regole create in questo modo sono considerate equivalenti a quelle create manualmente. Una regola creata da una finestra di dialogo può quindi essere meno specifica rispetto alla regola che ha attivato tale finestra di dialogo. Ciò significa che, dopo aver creato questo tipo di regola, la stessa operazione può attivare la stessa finestra.

Memorizza fino all'uscita dell'applicazione causa un'azione (**Consenti/Nega**) da utilizzare finché non verrà apportata una modifica alle regole o alla modalità di filtraggio oppure non verrà eseguito un aggiornamento del modulo HIPS o un riavvio del sistema. In seguito a una di queste tre azioni, le regole temporanee verranno eliminate.

4.1.5 Modalità giocatore

La modalità giocatore è una funzionalità pensata per gli utenti che richiedono un utilizzo ininterrotto del software, non desiderano essere disturbati dalle finestre popup e desiderano ridurre al minimo l'utilizzo della CPU. La modalità giocatore può essere utilizzata anche durante le presentazioni che non possono essere interrotte dall'attività antivirus. Attivando questa funzionalità, tutte le finestre popup vengono disattivate e l'attività di Pianificazione attività verrà completamente interrotta. La protezione del sistema è ancora in esecuzione in background ma non richiede alcun intervento da parte dell'utente.

È possibile attivare o disattivare la modalità giocatore nella finestra principale del programma in **Configurazione** > **Protezione computer** facendo clic su o accanto a **Modalità giocatore**. L'attivazione della modalità giocatore rappresenta un potenziale rischio per la protezione. Per tale motivo, l'icona relativa allo stato della protezione sulla barra delle attività diventa di colore arancione e viene visualizzato un avviso. Questo avviso verrà inoltre visualizzato nella finestra principale del programma dove **Modalità giocatore attivata** comparirà in arancione.

La modalità giocatore può essere attivata nella struttura Configurazione avanzata (F5) espandendo **Computer**, facendo clic su **Modalità giocatore** e selezionando la casella di controllo accanto a **Attiva modalità giocatore**.

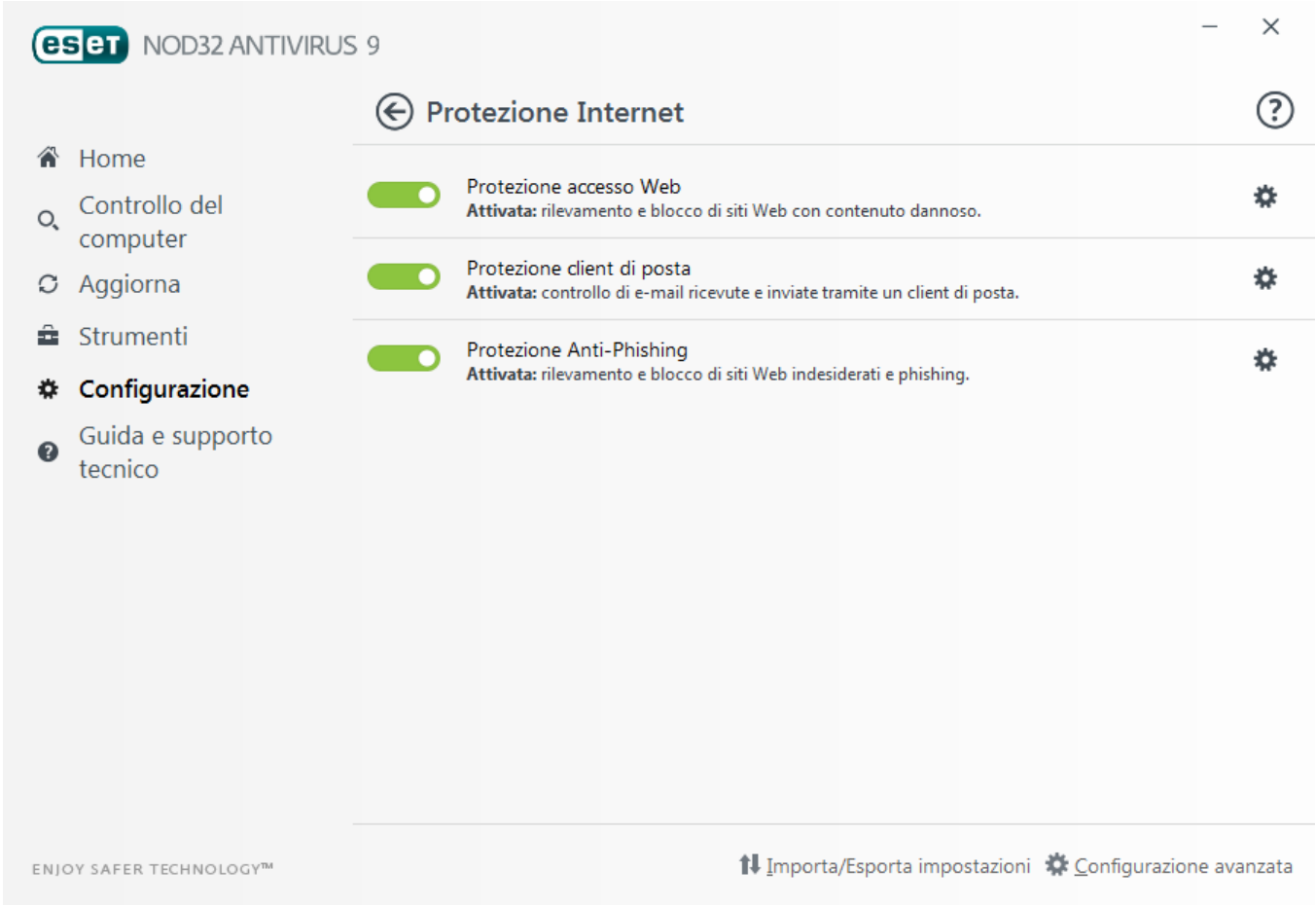
Selezionare **Attiva modalità giocatore quando vengono eseguite automaticamente applicazioni in modalità a schermo intero** in Configurazione avanzata (F5) per attivare la modalità giocatore all'avvio di un'applicazione in

modalità a schermo intero e interromperla all'uscita dall'applicazione.

Selezionare **Disattiva automaticamente modalità giocatore dopo** per definire l'intervallo di tempo dopo il quale la modalità giocatore verrà automaticamente disattivata.

4.2 Protezione Internet

Le opzioni di configurazione del Web ed e-mail sono disponibili nel riquadro **Configurazione** facendo clic su **Protezione Internet**. Da qui è possibile accedere a impostazioni del programma più dettagliate.



La connettività Internet è una funzione standard dei personal computer. Purtroppo, Internet è diventato lo strumento principale per la distribuzione di codice dannoso. Per questo motivo, è essenziale gestire attentamente le impostazioni di **Protezione accesso Web**.

Fare clic su per aprire le impostazioni di protezione Web/e-mail/anti-phishing in Configurazione avanzata.

La **Protezione client di posta** garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP. Utilizzando il programma plug-in per il client di posta in uso, ESET NOD32 Antivirus controlla tutte le comunicazioni da e verso il client di posta (POP3, MAPI, IMAP, HTTP).

La **Protezione Anti-Phishing** consente all'utente di bloccare le pagine Web che distribuiscono notoriamente contenuti phishing. Si consiglia vivamente di lasciare attivata l'opzione Anti-Phishing.

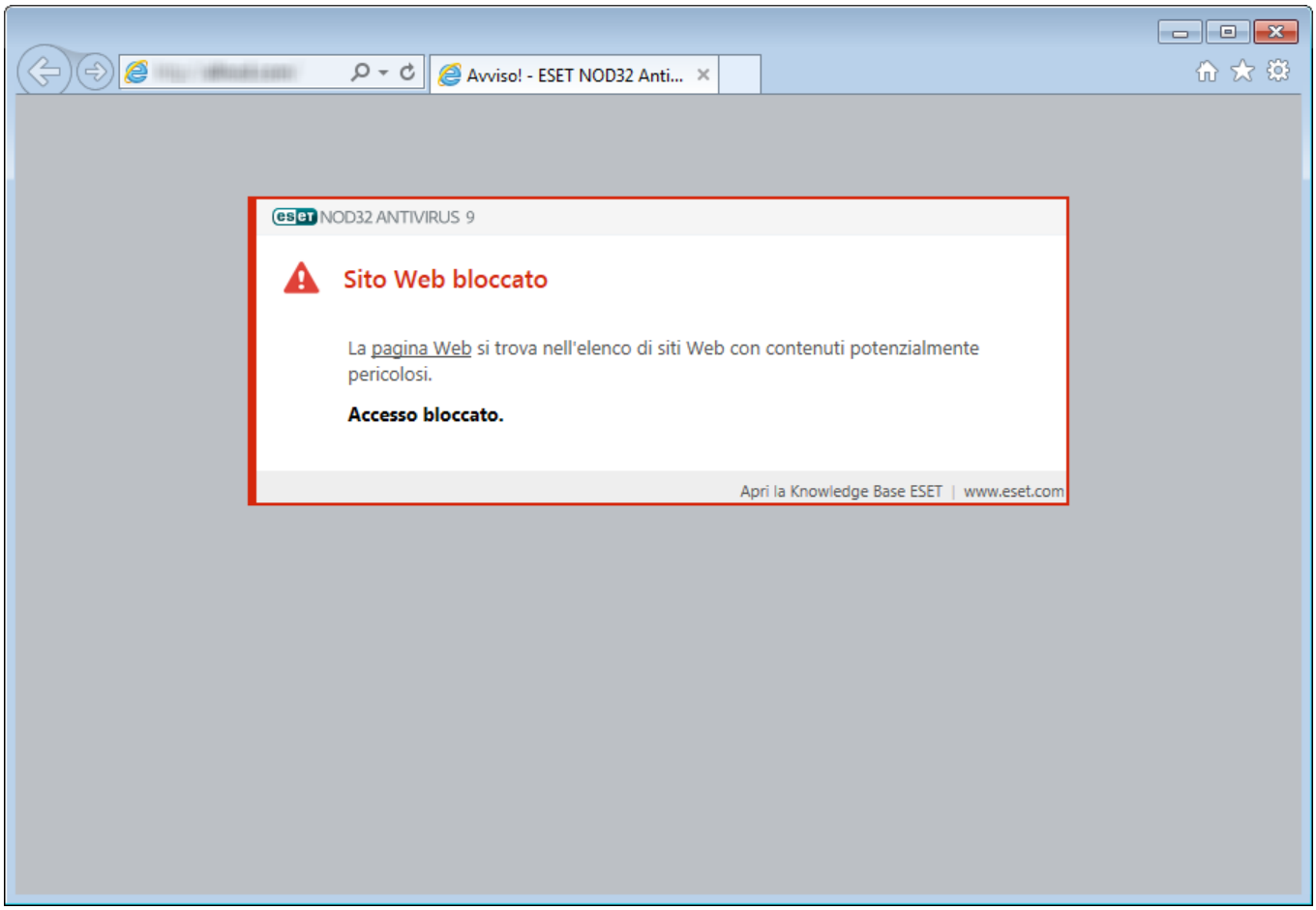
È possibile disattivare temporaneamente il modulo di protezione Web/e-mail Web/e-mail/anti-phishing facendo clic su .

4.2.1 Protezione accesso Web

La connettività Internet è una funzione standard in un personal computer. Purtroppo è diventato anche lo strumento principale per il trasferimento di codice dannoso. La Protezione accesso Web monitora la comunicazione tra i browser Web e i server remoti ed è conforme alle regole HTTP (Hypertext Transfer Protocol) e HTTPS (comunicazione crittografata).

L'accesso a pagine Web note per essere dannose è bloccato prima del download dei relativi contenuti. Tutte le altre pagine Web vengono controllate dal motore di controllo ThreatSense nel momento in cui vengono caricate e bloccate in caso di rilevamento di contenuti dannosi. La protezione accesso Web offre due livelli di protezione: il blocco in base alla blacklist e il blocco in base ai contenuti.

Si consiglia vivamente di attivare l'opzione Protezione accesso Web. L'opzione è disponibile dalla finestra principale di ESET NOD32 Antivirus accedendo a **Configurazione** > **Protezione Internet** > **Protezione accesso Web**.


Avviso! - ESET NOD32 Anti...
NOD32 ANTIVIRUS 9
Sito Web bloccato
La pagina Web si trova nell'elenco di siti Web con contenuti potenzialmente pericolosi.
Accesso bloccato.
Apri la Knowledge Base ESET | www.eset.com

Le seguenti opzioni sono disponibili in **Configurazione avanzata** (F5) > **Web ed e-mail** > **Protezione accesso Web**:

- **Protocolli Web**: consente all'utente di configurare il monitoraggio di questi protocolli standard utilizzati dalla maggior parte dei browser Internet.
- **Gestione indirizzi URL**: consente all'utente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo.
- **Parametri di ThreatSense**: configurazione avanzata scanner antivirus: consente all'utente di configurare impostazioni quali i tipi di oggetti da controllare (e-mail, archivi e così via.), i metodi di rilevamento della protezione accesso Web, ecc.

4.2.1.1 Di base

Attiva protezione accesso Web: se disattivata, la protezione accesso Web e la protezione Anti-Phishing non saranno garantite.

NOTA: si consiglia di lasciare attivata questa opzione.

4.2.1.2 Protocolli Web

Per impostazione predefinita, ESET NOD32 Antivirus è configurato per monitorare il protocollo HTTP utilizzato dalla maggior parte dei browser Internet.

Configurazione scanner HTTP

In Windows Vista e nelle versioni successive, il traffico HTTP viene monitorato sempre su tutte le porte di tutte le applicazioni. In Windows XP, è possibile modificare le **Porte utilizzate dal protocollo HTTP** in **Configurazione avanzata** (F5) > **Web ed e-mail** > **Protezione accesso Web** > **Protocolli Web**. Il traffico HTTP viene monitorato sulle porte specifiche di tutte le applicazioni e su tutte le porte delle applicazioni contrassegnate come Client Web e di posta.

Configurazione scanner HTTPS

ESET NOD32 Antivirus supporta anche il controllo del protocollo HTTPS. La comunicazione HTTPS utilizza un canale crittografato per trasferire le informazioni tra server e client. ESET NOD32 Antivirus controlla la comunicazione utilizzando i protocolli SSL (Secure Socket Layer) e TLS (Transport Layer Security). Il programma controllerà esclusivamente il traffico sulle porte definite in **Porte utilizzate dal protocollo HTTPS**, indipendentemente dalla versione del sistema operativo in uso.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare l'impostazione scanner, accedere a SSL/TLS nella sezione Configurazione avanzata, fare clic su **Web ed e-mail** > **SSL/TLS** e selezionare l'opzione **Attiva filtraggio protocollo SSL/TLS**.

4.2.1.3 Gestione indirizzo URL

La sezione Gestione indirizzo URL consente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo.

I siti Web presenti nell'**Elenco di indirizzi bloccati** non saranno accessibili a meno che non vengano anche inclusi nell'**Elenco di indirizzi consentiti**. Nei siti Web presenti nell'**Elenco di indirizzi esclusi dal controllo** non vengono ricercati codici dannosi al momento dell'accesso.

Se si desidera filtrare gli indirizzi HTTPS oltre alle pagine Web HTTP, è necessario selezionare **Attiva filtraggio protocollo SSL/TLS**. In caso contrario, verranno aggiunti solo i domini dei siti HTTPS visitati e non l'intero indirizzo URL.

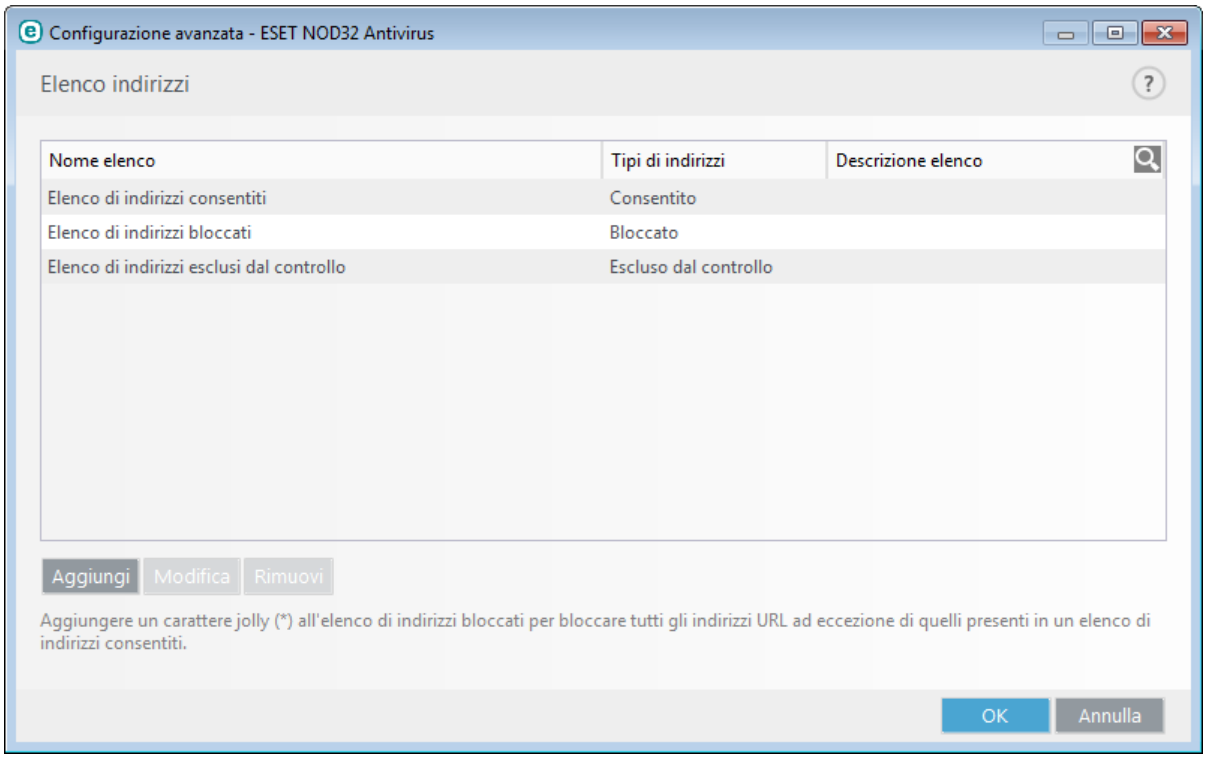
Se si aggiunge un indirizzo URL all'**Elenco indirizzi esclusi dal filtro**, l'indirizzo verrà escluso dal controllo. È inoltre possibile consentire o bloccare determinati indirizzi aggiungendoli all'**Elenco di indirizzi consentiti** o all'**Elenco di indirizzi bloccati**.

Se si desidera bloccare tutti gli indirizzi HTTP ad eccezione di quelli presenti nell'**Elenco di indirizzi consentiti** attivo, è necessario aggiungere * all'**Elenco di indirizzi bloccati** attivo.

Negli elenchi possono essere utilizzati i simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco sostituisce qualsiasi stringa di caratteri, mentre il punto interrogativo sostituisce qualsiasi simbolo. È necessario prestare particolare attenzione quando si specificano gli indirizzi esclusi, in quanto l'elenco dovrebbe contenere esclusivamente indirizzi affidabili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli * e ? siano utilizzati correttamente. Consultare Aggiungi indirizzo HTTP/maschera di dominio per ulteriori informazioni su come associare in maniera sicura un intero dominio, compresi tutti i sottodomini. Per attivare un elenco, selezionare **Elenco attivo**. Se si desidera ricevere una notifica relativa all'inserimento di un indirizzo contenuto nell'elenco corrente, selezionare **Notifica in caso di applicazione**.

SUGGERIMENTO: la gestione degli indirizzi URL consente inoltre di bloccare o consentire l'apertura di specifici tipi di

file mentre l'utente naviga in Internet. Ad esempio, se l'utente non desidera aprire file eseguibili, selezionare l'elenco dove si desidera bloccare questi file dal menu a discesa, quindi immettere la maschera "**.exe".



Elementi di controllo

Aggiungi: crea un nuovo elenco oltre a quelli predefiniti. Questa opzione è utile se si desidera suddividere vari gruppi di indirizzi in base a criteri logici. Ad esempio, un elenco di indirizzi bloccati potrebbe contenere indirizzi provenienti da una blacklist pubblica esterna e un altro la blacklist dell'utente. In tal modo, si facilita l'aggiornamento dell'elenco esterno mantenendo nel contempo intatto quello dell'utente.

Modifica: modifica gli elenchi esistenti. Utilizzare questa funzione per aggiungere o rimuovere indirizzi.

Rimuovi: rimuove gli elenchi esistenti. Questa funzione è disponibile esclusivamente per gli elenchi creati con **Aggiungi** e non per quelli predefiniti.

4.2.2 Protezione client di posta

4.2.2.1 Client di posta

L'integrazione di ESET NOD32 Antivirus con i client di posta aumenta il livello di protezione attiva contro codici dannosi nei messaggi di posta elettronica. Se il client di posta in uso è supportato, è possibile attivare l'integrazione in ESET NOD32 Antivirus. In caso di attivazione dell'integrazione, la barra degli strumenti di ESET NOD32 Antivirus viene inserita direttamente nel client di posta (ad eccezione di quella relativa alle versioni più recenti di Windows Live Mail), garantendo in tal modo una protezione più efficiente dei messaggi di posta elettronica. Le impostazioni relative all'integrazione sono disponibili sotto a **Configurazione** > **Configurazione avanzata** > **Web ed e-mail** > **Protezione client di posta** > **Client di posta**.

Integrazione con client di posta

I client di posta attualmente supportati sono Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. Per questi programmi, la protezione e-mail funziona come un plug-in. Il vantaggio principale offerto dal plug-in consiste nella sua indipendenza dal protocollo utilizzato. Quando il client di posta riceve un messaggio crittografato, questo viene decodificato e inviato allo scanner antivirus. Per un elenco completo dei client di posta supportati e delle relative versioni, consultare il seguente articolo della Knowledge Base ESET.

Anche se l'integrazione non è attivata, la comunicazione e-mail rimane comunque protetta tramite il modulo di protezione client di posta (POP3, IMAP).

Attivare **Disattiva il controllo alla modifica del contenuto della posta in arrivo** se si riscontra un rallentamento

del sistema durante l'utilizzo del client di posta (solo MS Outlook). Ciò può accadere durante il recupero di messaggi e-mail da Kerio Outlook Connector Store.

Messaggi e-mail da controllare

E-mail ricevuta: attiva/disattiva il controllo dei messaggi ricevuti.
E-mail inviata: attiva/disattiva il controllo dei messaggi inviati.
E-mail letta: attiva/disattiva il controllo dei messaggi letti.

Azione da eseguire sui messaggi e-mail infetti

Nessuna azione: se questa opzione è attivata, il programma identificherà gli allegati infetti senza tuttavia eseguire alcuna azione.
Elimina e-mail: il programma notificherà all'utente l'eventuale o le eventuali infiltrazioni ed eliminerà il messaggio.
Sposta e-mail nella cartella Posta eliminata: i messaggi e-mail infetti verranno spostati automaticamente nella cartella Posta eliminata.
Sposta e-mail nella cartella: i messaggi e-mail infetti verranno spostati automaticamente nella cartella specificata.

Cartella: specificare la cartella personalizzata in cui si desidera spostare i messaggi e-mail infetti una volta rilevati.

Ripeti controllo dopo l'aggiornamento: attiva/disattiva un nuovo controllo dopo l'aggiornamento del database delle firme antivirali.

Accetta i risultati del controllo da altri moduli: selezionando questa opzione, il modulo di protezione e-mail accetterà i risultati del controllo eseguito da altri moduli di protezione (controllo protocolli POP3, IMAP).

4.2.2.2 Protocolli e-mail

IMAP e POP3 sono i protocolli più comunemente utilizzati per ricevere comunicazioni e-mail in un'applicazione client di posta. IMAP (Internet Message Access Protocol) è un altro protocollo Internet per il recupero dei messaggi e-mail. Il protocollo IMAP offre alcuni vantaggi rispetto al protocollo POP3, tra cui, ad esempio, la possibilità di connettere simultaneamente più di un client alla stessa casella di posta e conservare informazioni sullo stato del messaggio (lettura, invio di risposta o eliminazione). ESET NOD32 Antivirus offre protezione per questi protocolli, indipendentemente dal client di posta utilizzato e senza richiedere la riconfigurazione del client di posta.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Il controllo del protocollo IMAP viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono controllate tutte le comunicazioni della porta 143, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

È possibile configurare il controllo dei protocolli IMAP/IMAPS e POP3/POP3S in Configurazione avanzata. Per accedere a questa impostazione, espandere **Web ed e-mail** > **Protezione client di posta** > **Protocolli e-mail**.

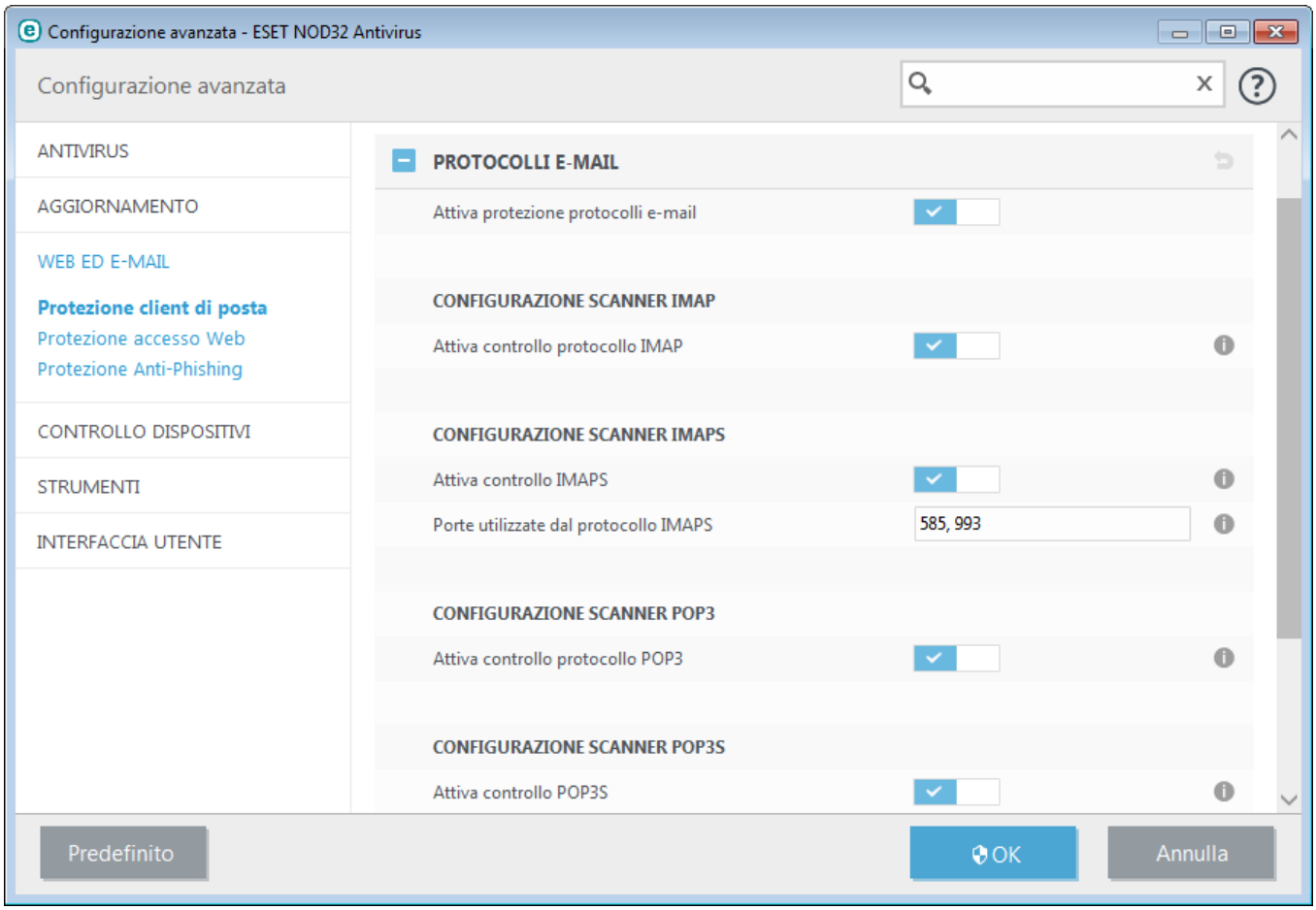
Attiva protezione protocolli e-mail: attiva il controllo dei protocolli di posta elettronica.

In Windows Vista e nelle versioni successive, i protocolli IMAP e POP3 vengono rilevati e controllati automaticamente su tutte le porte. In Windows XP, per tutte le applicazioni vengono controllate solo le **Porte utilizzate dal protocollo IMAP/POP3**, mentre per le applicazioni contrassegnate come Client Web e di posta vengono controllate tutte le porte.

ESET NOD32 Antivirus supporta anche il controllo dei protocolli IMAPS e POP3S che utilizzano un canale crittografato per trasferire le informazioni tra server e client. ESET NOD32 Antivirus controlla la comunicazione utilizzando i protocolli SSL (Secure Socket Layer) e TLS (Transport Layer Security). Il programma controllerà esclusivamente il traffico sulle porte definite in **Porte utilizzate dal protocollo HTTPS/POP3S**, indipendentemente dalla versione del sistema operativo utilizzato dall'utente.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare l'impostazione scanner, accedere a SSL/TLS nella sezione Configurazione avanzata, fare clic su **Web ed**

e-mail > **SSL/TLS** e selezionare l'opzione **Attiva filtraggio protocollo SSL/TLS**.



4.2.2.3 Avvisi e notifiche

La Protezione client di posta garantisce il controllo delle comunicazioni e-mail ricevute mediante i protocolli POP3 e IMAP. Utilizzando il plug-in per Microsoft Outlook e altri client e-mail, ESET NOD32 Antivirus controlla tutte le comunicazioni dal client e-mail (POP3, MAPI, IMAP, HTTP). Durante la verifica dei messaggi in arrivo, il programma utilizza tutti i metodi di controllo avanzato previsti nel motore di controllo ThreatSense. Ciò significa che il rilevamento di programmi dannosi viene eseguito ancora prima del confronto con il database delle firme antivirali. La scansione delle comunicazioni mediante i protocolli POP3 e IMAP non dipende dal client e-mail in uso.

Le opzioni di questa funzionalità sono disponibili in **Configurazione avanzata** sotto a **Web ed e-mail** > **Protezione client di posta** > **Avvisi e notifiche**.

Parametro ThreatSense: la configurazione avanzata dello scanner antivirus consente all'utente di configurare gli oggetti da controllare, i metodi di rilevamento e così via. Fare clic per visualizzare la finestra della configurazione dettagliata dello scanner antivirus.

Dopo che un messaggio e-mail è stato controllato, una notifica contenente i risultati di scansione può essere aggiunta al messaggio. È possibile scegliere le opzioni **Aggiungi notifiche all'e-mail ricevuta e letta**, **Aggiungi nota all'oggetto dell'e-mail infetta ricevuta e letta** o l'opzione **Aggiungi notifiche all'e-mail inviata**. Tenere presente che, in rare occasioni, le notifiche potrebbero essere omesse in messaggi HTML problematici o creati da malware. Le notifiche possono essere aggiunte sia alle e-mail ricevute e lette sia alle e-mail inviate. Le opzioni disponibili sono:

- **Mai** - Non viene aggiunta alcuna notifica.
- **Solo per l'e-mail infetta** - Solo i messaggi contenenti software dannoso vengono contrassegnati come controllati (impostazione predefinita).
- **Per tutte le e-mail** - Il programma aggiunge la notifica a tutte le e-mail sottoposte a scansione.

Aggiungi nota all'oggetto dell'e-mail infetta inviata: disattivare questa opzione se non si desidera che la protezione e-mail includa un avviso antivirus nell'oggetto di un'e-mail infetta. Questa funzione consente di filtrare in modo semplice le e-mail infette in base all'oggetto (se supportata dal programma e-mail in uso). Aumenta inoltre il livello

di credibilità del destinatario e, in caso di rilevamento di un'infiltrazione, fornisce informazioni utili sul livello di minaccia di un determinato messaggio e-mail o mittente.

Template aggiunto all'oggetto dell'e-mail infetta - Modificare questo template se si desidera cambiare il formato predefinito dell'oggetto di un'e-mail infetta. Questa funzione sostituirà l'oggetto del messaggio *"Ciao"* con un determinato valore predefinito *"[virus]"* nel seguente formato: *"[virus] Ciao"*. La variabile *%VIRUSNAME%* rappresenta la minaccia rilevata.

4.2.2.4 Integrazione con client e-mail

L'integrazione di ESET NOD32 Antivirus con i client e-mail aumenta il livello di protezione attiva contro codici dannosi nei messaggi e-mail. Se il client di posta in uso è supportato, è possibile attivare l'integrazione in ESET NOD32 Antivirus. In caso di attivazione dell'integrazione, la barra degli strumenti di ESET NOD32 Antivirus viene inserita direttamente nel client di posta, garantendo in tal modo una protezione e-mail più efficace. Le impostazioni di integrazione sono disponibili nella sezione **Configurazione** > **Accedi a configurazione avanzata...** > **Web ed e-mail** > **Protezione client e-mail** > **Integrazione con client e-mail**.

I client di posta attualmente supportati sono Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. Per un elenco completo dei client e-mail supportati e delle relative versioni, fare riferimento al seguente articolo della Knowledge Base ESET.

Selezionare la casella di controllo accanto a **Disattiva il controllo alla modifica del contenuto della posta in arrivo** se si riscontra un rallentamento del sistema durante l'utilizzo del client di posta. Ciò può accadere durante il recupero di e-mail da Kerio Outlook Connector Store.

Anche se l'integrazione non è attivata, la comunicazione e-mail rimane comunque protetta tramite il modulo di protezione client e-mail (POP3, IMAP).

4.2.2.4.1 Configurazione della protezione client di posta

Il modulo di protezione client di posta supporta i seguenti client di posta: Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. Per questi programmi la protezione e-mail esegue la stessa funzione di un plugin. Il vantaggio principale offerto dal plugin consiste nella sua indipendenza dal protocollo utilizzato. Quando il client di posta riceve un messaggio crittografato, questo viene decodificato e inviato al programma di scanner antivirus.

4.2.2.5 Filtro POP3, POP3S

Il protocollo POP3 è quello più diffuso per la ricezione di comunicazioni e-mail in un'applicazione client e-mail. ESET NOD32 Antivirus offre la protezione per questo protocollo, indipendentemente dal client e-mail in uso.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Perché il modulo funzioni correttamente, verificare che sia attivato: il controllo del protocollo POP3 viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono sottoposte a scansione tutte le comunicazioni della porta 110, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare l'impostazione scanner, accedere a SSL/TLS nella sezione Configurazione avanzata, fare clic su **Web ed e-mail** > **SSL/TLS** e selezionare l'opzione **Attiva filtraggio protocollo SSL/TLS**.

In questa sezione è possibile configurare il controllo dei protocolli POP3 e POP3S.

Attiva controllo e-mail - Se questa opzione è attivata, tutto il traffico POP3 viene monitorato per rilevare il software dannoso.

Porte utilizzate dal protocollo POP3 - Elenco delle porte usate dal protocollo POP3 (110 per impostazione predefinita).

ESET NOD32 Antivirus supporta anche il controllo del protocollo POP3S. Questo tipo di comunicazione utilizza un canale crittografato per trasferire le informazioni tra server e client. ESET NOD32 Antivirus controlla le comunicazioni utilizzando i metodi di crittografia SSL (Secure Socket Layer) e TLS (Transport Layer Security).

Non effettuare il controllo POP3S - La comunicazione crittografata non verrà controllata.

Effettua controllo protocollo POP3S per le porte selezionate - Selezionare questa opzione per attivare il controllo POP3S solo per le porte definite in **Porte utilizzate dal protocollo POP3S**.

Porte utilizzate dal protocollo POP3S - Elenco delle porte POP3S da controllare (995 per impostazione predefinita).

4.2.3 Filtraggio protocolli

La protezione antivirus per i protocolli delle applicazioni viene offerta dal motore di controllo ThreatSense, che integra perfettamente tutte le tecniche di controllo avanzato dei malware. Il filtraggio protocolli funziona automaticamente, indipendentemente dal browser Internet o dal client di posta in uso. Per modificare le impostazioni crittografate (SSL/TLS), accedere a **Web ed e-mail** > **SSL/TLS**.

Attiva filtraggio contenuto protocollo applicazioni: può essere utilizzato per disattivare il filtraggio dei protocolli. Tenere presente che il funzionamento di numerosi componenti di ESET NOD32 Antivirus (protezione accesso Web, protezione protocolli e-mail, Anti-Phishing, controllo Web) dipende interamente da questa funzione.

Applicazioni escluse: consente all'utente di escludere applicazioni specifiche dal filtraggio protocolli. Questa funzione è utile in caso di problemi di compatibilità causati dal filtraggio protocolli.

Indirizzi IP esclusi: consente all'utente di escludere indirizzi remoti specifici dal filtraggio protocolli. Questa funzione è utile in caso di problemi di compatibilità causati dal filtraggio protocolli.

Client Web e di posta: questa funzione, utilizzata solo sui sistemi operativi Windows XP, consente all'utente di selezionare le applicazioni per cui l'intero traffico viene filtrato dalla funzione di filtraggio protocolli, indipendentemente dalle porte utilizzate.

4.2.3.1 Web e client di posta

NOTA: in Windows Vista Service Pack 1 e Windows Server 2008 per il controllo delle comunicazioni di rete viene utilizzata la nuova architettura Windows Filtering Platform (WFP). Poiché la tecnologia WPF utilizza speciali tecniche di monitoraggio, la sezione **Web e client di posta** non è disponibile.

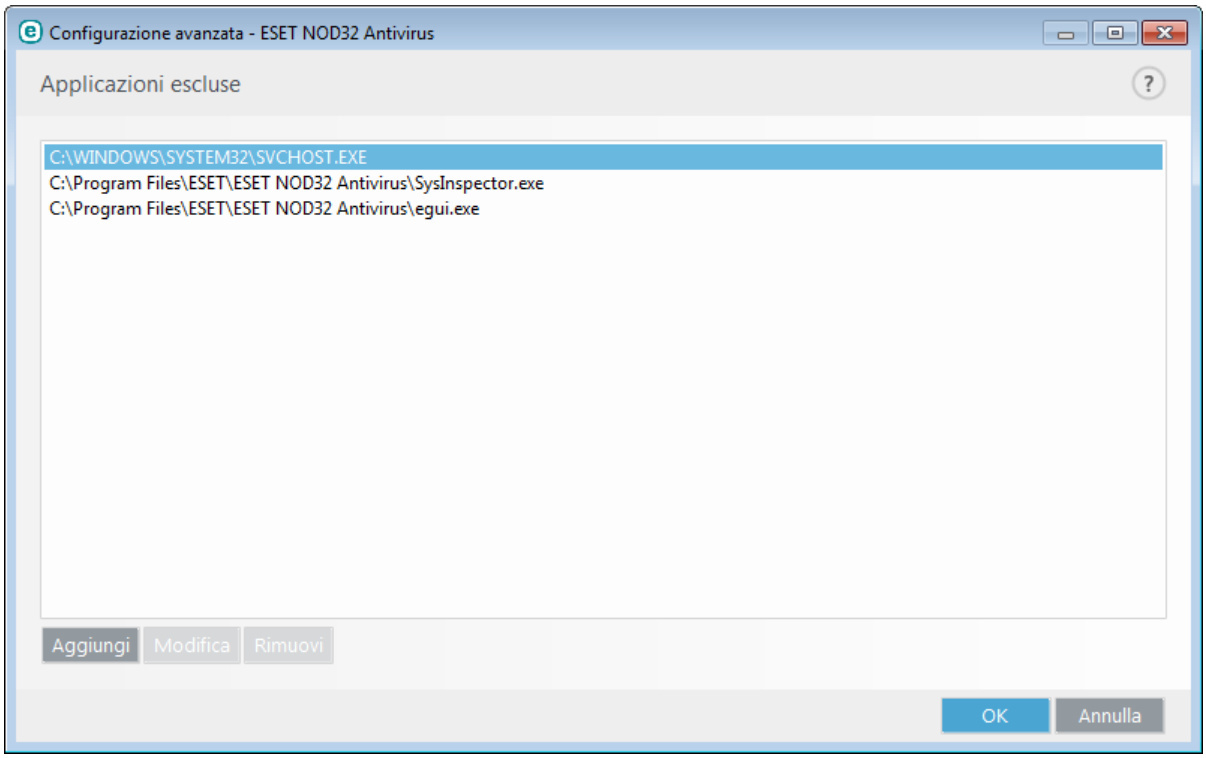
A causa dell'enorme quantità di codice dannoso che circola su Internet, una navigazione Internet sicura è essenziale per la protezione del computer. Le vulnerabilità dei browser Web e i collegamenti fraudolenti aiutano il codice dannoso a penetrare inosservato nel sistema. Per tale motivo, ESET NOD32 Antivirus si focalizza sulla sicurezza dei browser Web. Ogni applicazione che accede alla rete può essere contrassegnata come un browser. La casella di controllo presenta due stati:

- **Deselezionata** - La comunicazione delle applicazioni viene filtrata solo per le porte specificate.
- **Selezionata** - La comunicazione viene sempre filtrata (anche se viene impostata una porta differente).

4.2.3.2 Applicazioni escluse

Per escludere la comunicazione di specifiche applicazioni di rete dal filtraggio dei contenuti, selezionarle nell'elenco. Sulla comunicazione HTTP/POP3/IMAP delle applicazioni selezionate non verrà eseguito il rilevamento delle minacce. È consigliabile usare questa opzione solo per le applicazioni che non funzionano correttamente se la rispettiva comunicazione viene sottoposta a controllo.

L'esecuzione di applicazioni e servizi sarà disponibile automaticamente. Fare clic su **Aggiungi** per aggiungere manualmente un'applicazione non visualizzata nell'elenco del filtraggio protocolli.

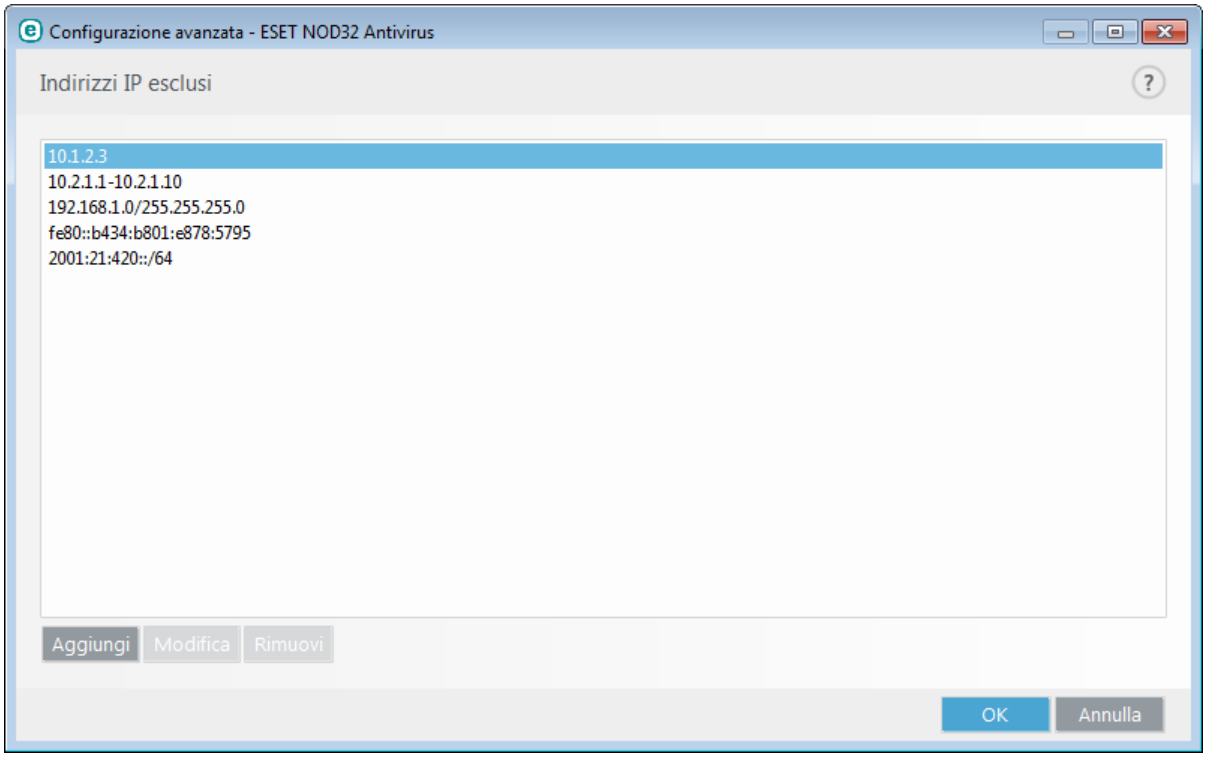


4.2.3.3 Indirizzi IP esclusi

Le voci presenti nell'elenco saranno escluse dal filtraggio del contenuto del protocollo. Sulla comunicazione HTTP/POP3/IMAP da/verso gli indirizzi selezionati non verrà eseguito il rilevamento delle minacce. È consigliabile utilizzare questa opzione solo per gli indirizzi di cui è nota l'affidabilità.

Fare clic su **Aggiungi** per escludere un indirizzo IP/intervallo di indirizzi/subnet di un punto remoto non visualizzato sull'elenco del filtro protocolli.

Fare clic su **Rimuovi** per rimuovere le voci selezionate dall'elenco.



4.2.3.3.1 Aggiungi indirizzo IPv4

Ciò consente di aggiungere un indirizzo/intervallo di indirizzi/subnet IP di un punto remoto a cui si applica la regola. Sebbene sia il più vecchio, il protocollo Internet versione 4 è quello maggiormente utilizzato.

Indirizzo singolo - Aggiunge l'indirizzo IP di un singolo computer a cui deve essere applicata la regola, ad esempio *192.168.0.10*.

Intervallo di indirizzi - Immettere il primo e l'ultimo indirizzo IP per specificare l'intervallo IP (di più computer) per cui deve essere applicata la regola, ad esempio da *192.168.0.1* a *192.168.0.99*.

Subnet - Subnet (gruppo di computer) definita da un indirizzo IP e da una maschera.

Ad esempio, *255.255.255.0* è la maschera di rete per il prefisso *192.168.1.0/24*, che indica l'intervallo di indirizzi compreso tra *192.168.1.1* e *192.168.1.254*.

4.2.3.3.2 Aggiungi indirizzo IPv6

Ciò consente di aggiungere un indirizzo/una subnet IPv6 di un punto remoto a cui si applica la regola. Si tratta della versione più recente del protocollo Internet e sostituirà la versione precedente 4.

Indirizzo singolo - Aggiunge l'indirizzo IP di un singolo computer a cui deve essere applicata la regola, ad esempio *2001:718:1c01:16:214:22ff:fec9:ca5*.

Subnet - Subnet (gruppo di computer) definita da un indirizzo IP e da una maschera, ad esempio *2002:c0a8:6301:1::1/64*).

4.2.3.4 SSL/TLS

ESET NOD32 Antivirus è in grado di ricercare le minacce contenute nelle comunicazioni che utilizzano il protocollo SSL. È possibile utilizzare varie modalità di controllo per l'analisi delle comunicazioni protette dal protocollo SSL con certificati attendibili, certificati sconosciuti o certificati che sono esclusi dal controllo delle comunicazioni protette dal protocollo SSL.

Attiva filtraggio protocollo SSL/TLS: se il filtraggio protocolli è disattivato, il programma non controllerà le comunicazioni sull'SSL.

La **Modalità filtraggio protocollo SSL/TLS** è disponibile nelle seguenti opzioni:

Modalità automatica: la modalità automatica eseguirà il controllo esclusivamente delle applicazioni appropriate quali i browser Web e i client di posta. È possibile ignorare questa funzione selezionando le applicazioni per le quali le comunicazioni verranno sottoposte al controllo.

Modalità interattiva: all'accesso a un nuovo sito protetto da SSL (con un certificato sconosciuto), viene visualizzata una finestra di dialogo per la scelta dell'azione. Questa modalità consente di creare un elenco di certificati SSL che verranno esclusi dal controllo.

Modalità criteri: selezionare questa opzione per controllare tutte le comunicazioni protette dal protocollo SSL ad eccezione delle comunicazioni protette dai certificati esclusi dal controllo. Se viene stabilita una nuova comunicazione usando un certificato firmato sconosciuto, all'utente non verrà inviata alcuna notifica e la comunicazione verrà filtrata in modo automatico. Quando si accede a un server con un certificato non attendibile contrassegnato come attendibile (presente nell'elenco dei certificati attendibili), la comunicazione con il server è consentita e il contenuto del canale di comunicazione viene filtrato.

Elenco di applicazioni filtrate tramite SSL: consente all'utente di personalizzare il comportamento di ESET NOD32 Antivirus per specifiche applicazioni.

Elenco di certificati noti: consente all'utente di personalizzare il comportamento di ESET NOD32 Antivirus per specifici certificati SSL.

Escludi comunicazioni protette con certificati con validità estesa (EV): se questa opzione è attivata, la comunicazione con questo tipo di certificato SSL sarà esclusa dal controllo. I certificati SSL con validità estesa assicurano all'utente che sta visitando il sito Web desiderato e non un sito contraffatto assolutamente identico a quello desiderato (in genere i siti di phishing).

Blocca le comunicazioni crittografate che utilizzano il protocollo obsoleto SSL v2 - La comunicazione che utilizza la versione precedente del protocollo SSL verrà automaticamente bloccata.

Certificato radice

Aggiungi il certificato radice ai browser conosciuti: affinché la comunicazione SSL funzioni in modo adeguato nei browser/client di posta dell'utente, è fondamentale che il certificato radice di ESET venga aggiunto all'elenco dei certificati radice noti (autori). Quando questa opzione è attivata, ESET NOD32 Antivirus aggiungerà automaticamente il certificato radice di ESET ai browser conosciuti (ad esempio, Opera e Firefox). Per i browser che utilizzano l'archivio di certificazioni di sistema, il certificato viene aggiunto automaticamente (ad esempio, Internet Explorer).

Per applicare il certificato a browser non supportati, fare clic su **Visualizza certificato** > **Dettagli** > **Copia su file...** e importarlo manualmente nel browser.

Validità del certificato

Se il certificato non può essere verificato mediante l'utilizzo dell'archivio certificati TRCA: in alcuni casi, non è possibile verificare la validità del certificato di un sito Web utilizzando l'archivio Autorità di certificazione radice attendibili (TRCA). Ciò significa che il certificato è firmato da qualcuno (ad esempio, l'amministratore di un server Web o di una piccola azienda) e considerare questo certificato come attendibile non rappresenta sempre un rischio per la sicurezza. Gran parte delle aziende di grandi dimensioni (ad esempio, le banche) utilizza un certificato firmato dal TRCA. Dopo aver selezionato **Chiedi conferma della validità dei certificati** (impostazione predefinita), all'utente verrà richiesto di selezionare un'azione da eseguire in caso di comunicazione

crittografata. È possibile selezionare **Blocca comunicazioni che utilizzano il certificato** per terminare sempre le connessioni crittografate ai siti con certificati non verificati.

Se il certificato è danneggiato o non valido: ciò significa che il certificato è scaduto o che la firma era errata. In questo caso, è consigliabile lasciare selezionata l'opzione **Blocca comunicazioni che utilizzano il certificato**.

4.2.3.4.1 Certificati

Affinché le comunicazioni SSL funzionino in modo adeguato nei browser/client di posta, è fondamentale che il certificato radice per ESET sia aggiunto all'elenco dei certificati radice noti (autori). È necessario attivare **Aggiungi il certificato radice ai browser conosciuti**. Selezionare questa opzione per aggiungere automaticamente il certificato radice di ESET ai browser conosciuti (ad esempio, Opera e Firefox). Per i browser che utilizzano l'archivio di certificazioni di sistema, il certificato viene aggiunto automaticamente (ad esempio, Internet Explorer). Per applicare il certificato a browser non supportati, fare clic su **Visualizza certificato** > **Dettagli** > **Copia su file...**, quindi importarlo manualmente nel browser.

In alcuni casi non è possibile verificare la validità del certificato mediante l'archivio Autorità di certificazione radice attendibili (ad esempio VeriSign). Ciò significa che il certificato è auto-firmato da qualcuno (ad esempio, l'amministratore di un server Web o una piccola azienda) e considerare questo certificato come attendibile non rappresenta sempre un rischio per la sicurezza. La maggior parte delle principali aziende (ad esempio, le banche) utilizza un certificato firmato da TRCA. Dopo aver selezionato **Chiedi conferma della validità dei certificati** (impostazione predefinita), all'utente verrà richiesto di selezionare un'azione da eseguire in caso di comunicazione crittografata. Verrà visualizzata una finestra di dialogo in cui l'utente potrà scegliere se contrassegnare il certificato come attendibile o escluso. Nel caso in cui il certificato non sia presente nell'elenco TRCA, la finestra sarà rossa. In caso contrario, sarà di colore verde.

È possibile selezionare **Blocca la comunicazione che utilizza il certificato** per terminare sempre una connessione crittografata al sito che utilizza il certificato non verificato.

Se il certificato non è valido oppure è danneggiato, significa che è scaduto o che l'auto-firma era errata. In questo caso, è consigliabile bloccare la comunicazione che utilizza il certificato.

4.2.3.4.2 Elenco di certificati noti

L'**Elenco di certificati noti** può essere utilizzato per la personalizzazione del comportamento di ESET NOD32 Antivirus per specifici certificati SSL e per ricordare le azioni scelte se in **Modalità filtraggio protocollo SSL/TSL** viene selezionata la **Modalità interattiva**. L'elenco può essere visualizzato e modificato in **Configurazione avanzata** (F5) > **Web e e-mail** > **SSL/TLS** > **Elenco di certificati noti**.

La finestra **Elenco di certificati noti** è formata da:

Colonne

Nome : nome del certificato.

Autorità di certificazione emittente: nome del creatore del certificato.

Oggetto certificato: campo dell'oggetto che identifica l'entità associata alla chiave pubblica archiviata nel campo Chiave pubblica dell'oggetto.

Accesso : selezionare **Consenti** o **Blocca** come **Azione di accesso** per consentire/bloccare la comunicazione protetta da questo certificato indipendentemente dalla sua attendibilità. Selezionare **Auto** per consentire i certificati attendibili e richiedere quelli inattendibili. Selezionare **Chiedi** per chiedere sempre all'utente cosa fare.

Controlla : selezionare **Controlla** o **Ignora** come **Azione di controllo** per controllare o ignorare la comunicazione protetta da questo certificato. Selezionare **Auto** per eseguire il controllo in modalità automatica e attivare la richiesta in modalità interattiva. Selezionare **Chiedi** per chiedere sempre all'utente cosa fare.

Elementi di controllo

Modifica: selezionare il certificato che si desidera configurare e fare clic su **Modifica**.

Rimuovi: selezionare il certificato che si desidera eliminare e fare clic su **Rimuovi**.

OK/Annulla: fare clic su **OK** se si desidera salvare le modifiche o su **Annulla** per uscire senza salvare.

4.2.3.4.3 Elenco di applicazioni filtrate tramite SSL

L'**Elenco di applicazioni filtrate tramite SSL** può essere utilizzato per la personalizzazione del comportamento di ESET NOD32 Antivirus per specifiche applicazioni e per ricordare le azioni scelte se in **Modalità filtraggio protocollo SSL** viene selezionata la **Modalità interattiva**. L'elenco può essere visualizzato e modificato in **Configurazione avanzata** (F5) > **Web e e-mail** > **SSL/TLS** > **Elenco di applicazioni filtrate tramite SSL**.

La finestra **Elenco di applicazioni filtrate tramite SSL** è formata da:

Colonne

Applicazione : nome dell'applicazione.

Azione di controllo : selezionare **Controlla** o **Ignora** per controllare o ignorare la comunicazione. Selezionare **Auto** per eseguire il controllo in modalità automatica e attivare la richiesta in modalità interattiva. Selezionare **Chiedi** per chiedere sempre all'utente cosa fare.

Elementi di controllo

Aggiungi : consente di aggiungere l'applicazione filtrata.

Modifica: selezionare il certificato che si desidera configurare e fare clic su **Modifica**.

Rimuovi: selezionare il certificato che si desidera eliminare e fare clic su **Rimuovi**.

OK/Annulla: fare clic su **OK** se si desidera salvare le modifiche o su **Annulla** per uscire senza salvare.

4.2.4 Protezione Anti-Phishing

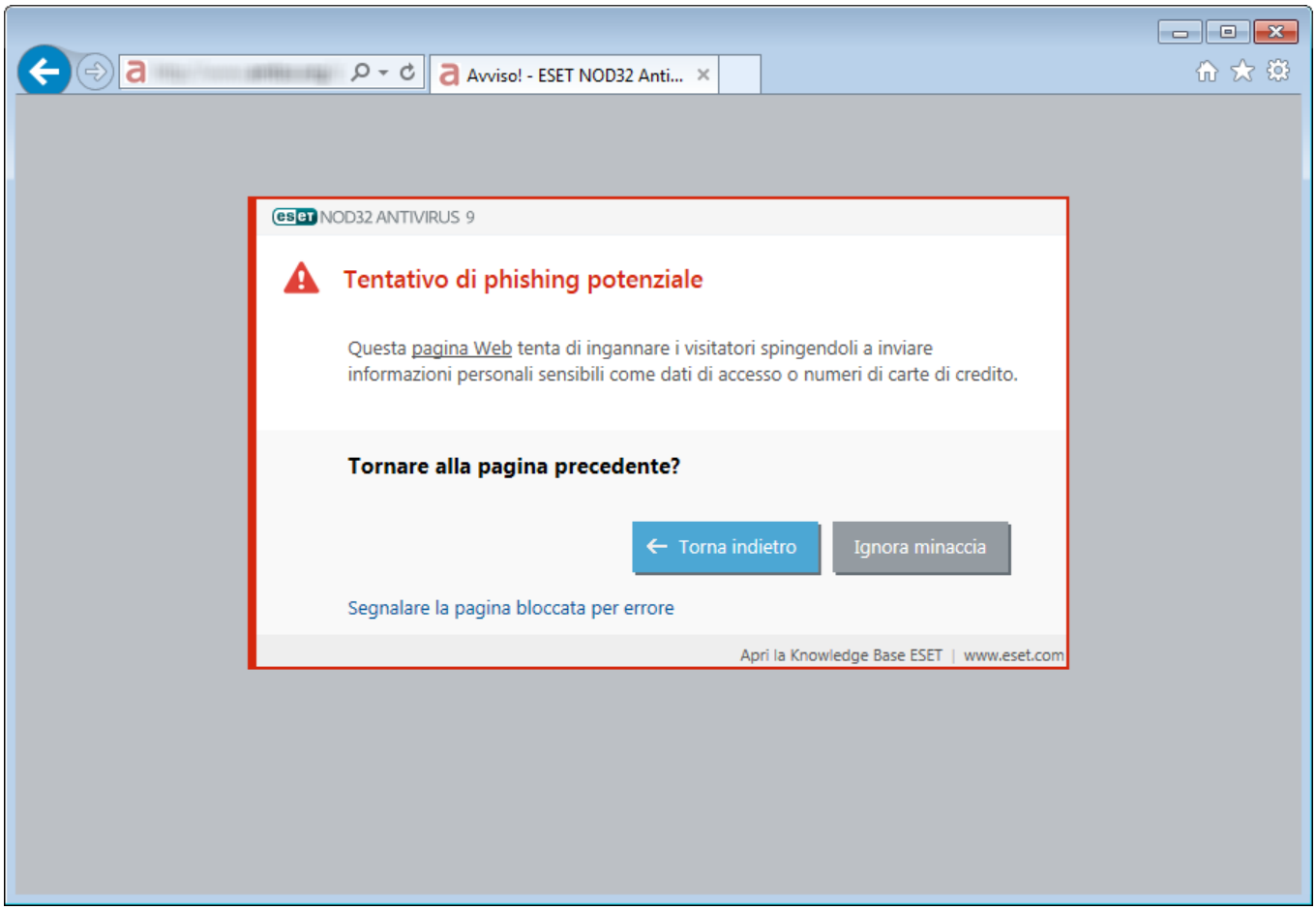
Il termine phishing definisce un'attività illegale che si avvale dell'ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni riservate). Il phishing viene spesso utilizzato per ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via. Per ulteriori informazioni su questa attività, consultare il glossario. ESET NOD32 Antivirus integra sistemi di protezione anti-phishing, ovvero una funzione che blocca pagine Web note per distribuire questo tipo di contenuto.

Si consiglia vivamente di attivare la funzione Anti-Phishing in ESET NOD32 Antivirus. A tale scopo, aprire **Configurazione avanzata** (F5) e accedere a **Web ed e-mail** > **Protezione Anti-Phishing**.

Consultare l'articolo della Knowledge Base per ulteriori informazioni sulla protezione Anti-Phishing in ESET NOD32 Antivirus.

Accesso ad un sito Web phishing

Accedendo a un sito Web phishing riconosciuto, nel browser Web in uso comparirà la seguente finestra di dialogo. Se si desidera ancora accedere al sito Web, fare clic su **Ignora minaccia** (scelta non consigliata).


Avviso! - ESET NOD32 Anti...
NOD32 ANTIVIRUS 9
Tentativo di phishing potenziale
Questa pagina Web tenta di ingannare i visitatori spingendoli a inviare informazioni personali sensibili come dati di accesso o numeri di carte di credito.
Tornare alla pagina precedente?
Torna indietro
Ignora minaccia
Segnalare la pagina bloccata per errore
Apri la Knowledge Base ESET | www.eset.com

NOTA: per impostazione predefinita, i potenziali siti Web phishing che sono stati inseriti nella whitelist scadranno dopo alcune ore. Per consentire un sito Web in modo permanente, utilizzare lo strumento Gestione indirizzi URL. Da **Configurazione avanzata** (F5), espandere **Web ed e-mail** > **Protezione accesso Web** > **Gestione indirizzi URL** > **Elenco indirizzi**, fare clic su **Modifica** e aggiungere all'elenco il sito Web che si desidera modificare.

Segnalazione di un sito phishing

Il collegamento Segnala consente di segnalare un sito Web phishing/dannoso a ESET ai fini dell'analisi.

NOTA: prima di inviare un sito Web a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:
- il sito Web non viene rilevato,
- il sito Web viene erroneamente rilevato come una minaccia. In questo caso, è possibile Segnalare la pagina bloccata per errore.

In alternativa, è possibile inviare il sito Web tramite e-mail. Inviare l'e-mail a campioni@eset.com. Ricordare di utilizzare un oggetto descrittivo e di fornire il maggior numero di informazioni possibile sul sito Web (ad esempio, il sito Web che ha condotto l'utente sulla pagina in questione, come si è venuti a conoscenza del sito Web, ecc.).

4.3 Aggiornamento del programma

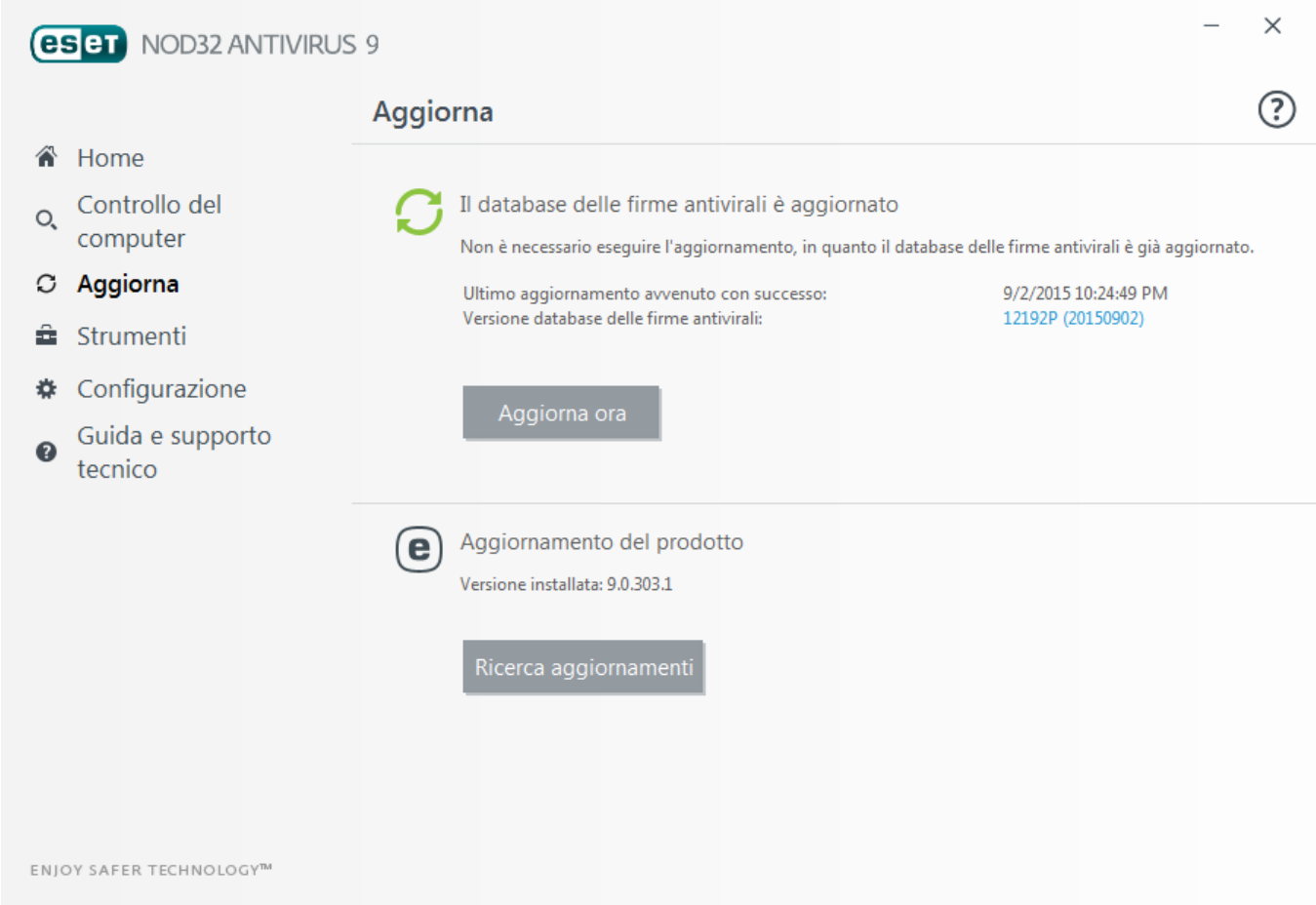
L'aggiornamento periodico di ESET NOD32 Antivirus rappresenta il metodo migliore per garantire il livello massimo di protezione del computer. Il modulo di aggiornamento garantisce in due modi che il programma sia sempre aggiornato: attraverso l'aggiornamento rispettivamente del database delle firme antivirali e dei componenti del sistema.

Facendo clic su **Aggiorna** nella finestra principale del programma, è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente e valutare se sia necessario un aggiornamento. Nella finestra principale sono inoltre contenute informazioni sulla versione del database delle firme antivirali. Questo indicatore numerico rappresenta un collegamento attivo al sito Web di ESET, in cui vengono riportate tutte le firme aggiunte nel corso dell'aggiornamento in questione.

Oltre agli aggiornamenti automatici, è possibile fare clic su **Aggiorna adesso** per avviare un aggiornamento

manualmente. L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per garantire una protezione completa contro codici dannosi. È opportuno prestare particolare attenzione alla relativa configurazione e al funzionamento. Per ricevere gli aggiornamenti, è necessario attivare il prodotto tramite la Chiave di licenza. Se durante l'installazione non è stata eseguita questa operazione, è possibile inserire la chiave di licenza per attivare il prodotto durante l'aggiornamento per accedere ai server di aggiornamento ESET.

NOTA: la chiave di licenza viene inviata tramite e-mail da ESET dopo l'acquisto di ESET NOD32 Antivirus.



Ultimo aggiornamento riuscito - Data dell'ultimo aggiornamento. Se non viene visualizzata una data recente, il database delle firme antivirali potrebbe non essere aggiornato.

Versione del database delle firme antivirali - Numero del database delle firme antivirali, che rappresenta anche un collegamento attivo al sito Web ESET. Selezionare questa opzione per visualizzare un elenco di tutte le firme aggiunte in un aggiornamento specifico.

Fare clic su **Ricerca aggiornamenti** per verificare la disponibilità della versione di ESET NOD32 Antivirus più recente.

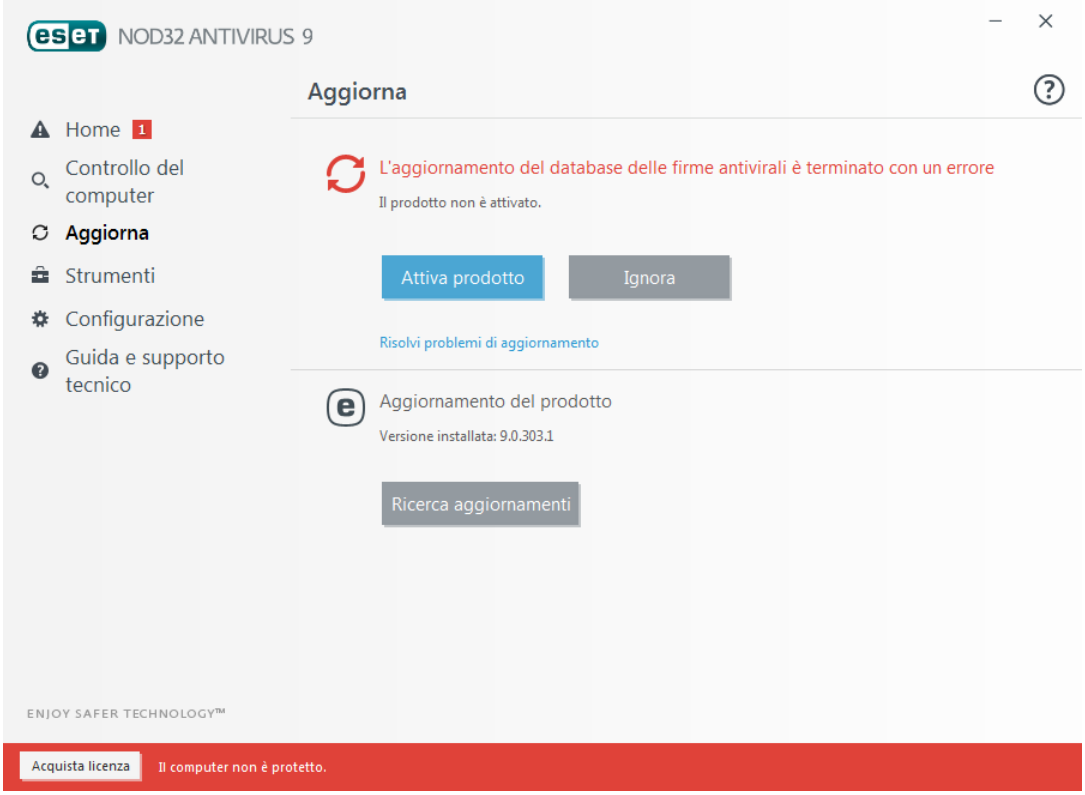
Processo di aggiornamento

Dopo aver selezionato **Aggiorna ora**, verrà avviato il download. Verranno visualizzati una barra di avanzamento del download e il tempo rimanente per il completamento dell'operazione. Per interrompere l'aggiornamento, fare clic su **Annulla l'aggiornamento**.

Importante: in circostanze normali, nella finestra **Aggiorna** viene visualizzato il messaggio **Aggiornamento non necessario. Il database delle firme antivirali è aggiornato**. In caso contrario, il programma è obsoleto ed è maggiormente esposto alle infezioni. Aggiornare il database delle firme antivirali appena possibile. In caso contrario, viene visualizzato uno dei seguenti messaggi:

Il messaggio di notifica precedente è correlato ai due messaggi **Aggiornamento del database delle firme antivirali terminato con un errore** seguenti, relativi agli aggiornamenti non riusciti:

1. **Licenza non valida**: la chiave di licenza non è stata inserita correttamente durante la configurazione dell'aggiornamento. Si consiglia di verificare i dati di autenticazione. Nella finestra Configurazione avanzata (fare clic su **Configurazione** nel menu principale, quindi su **Configurazione avanzata** oppure premere F5 sulla tastiera), sono disponibili ulteriori opzioni di aggiornamento. Fare clic su **Guida e supporto tecnico** > **Modifica licenza** nel menu principale per inserire una nuova chiave di licenza.
2. **Si è verificato un errore durante il download dei file di aggiornamento**: questo errore potrebbe essere causato da Impostazioni di connessione Internet non corrette. Si consiglia di verificare la connettività Internet (aprendo un qualsiasi sito Web nel browser). Se il sito Web non si apre, è possibile che la connessione Internet non sia presente o che si siano verificati problemi di connettività nel computer in uso. Se la connessione Internet non è attiva, contattare il proprio Provider di servizi Internet (ISP).



NOTA: per ulteriori informazioni, consultare questo articolo della Knowledge Base ESET.

4.3.1 Impostazioni di aggiornamento

Le opzioni di configurazione degli aggiornamenti sono disponibili nella struttura **Configurazione avanzata** (F5) sotto a **Aggiornamento** > **Di base**. Questa sezione consente di specificare informazioni sull'origine degli aggiornamenti, come ad esempio i server di aggiornamento e i dati per l'autenticazione di tali server.

Generale

Il profilo di aggiornamento attualmente in uso viene visualizzato nel menu a discesa **Profilo selezionato**. Per creare un nuovo profilo, fare clic su **Modifica** accanto a **Elenco di profili**, inserire il proprio **Nome profilo**, quindi fare clic su **Aggiungi**.

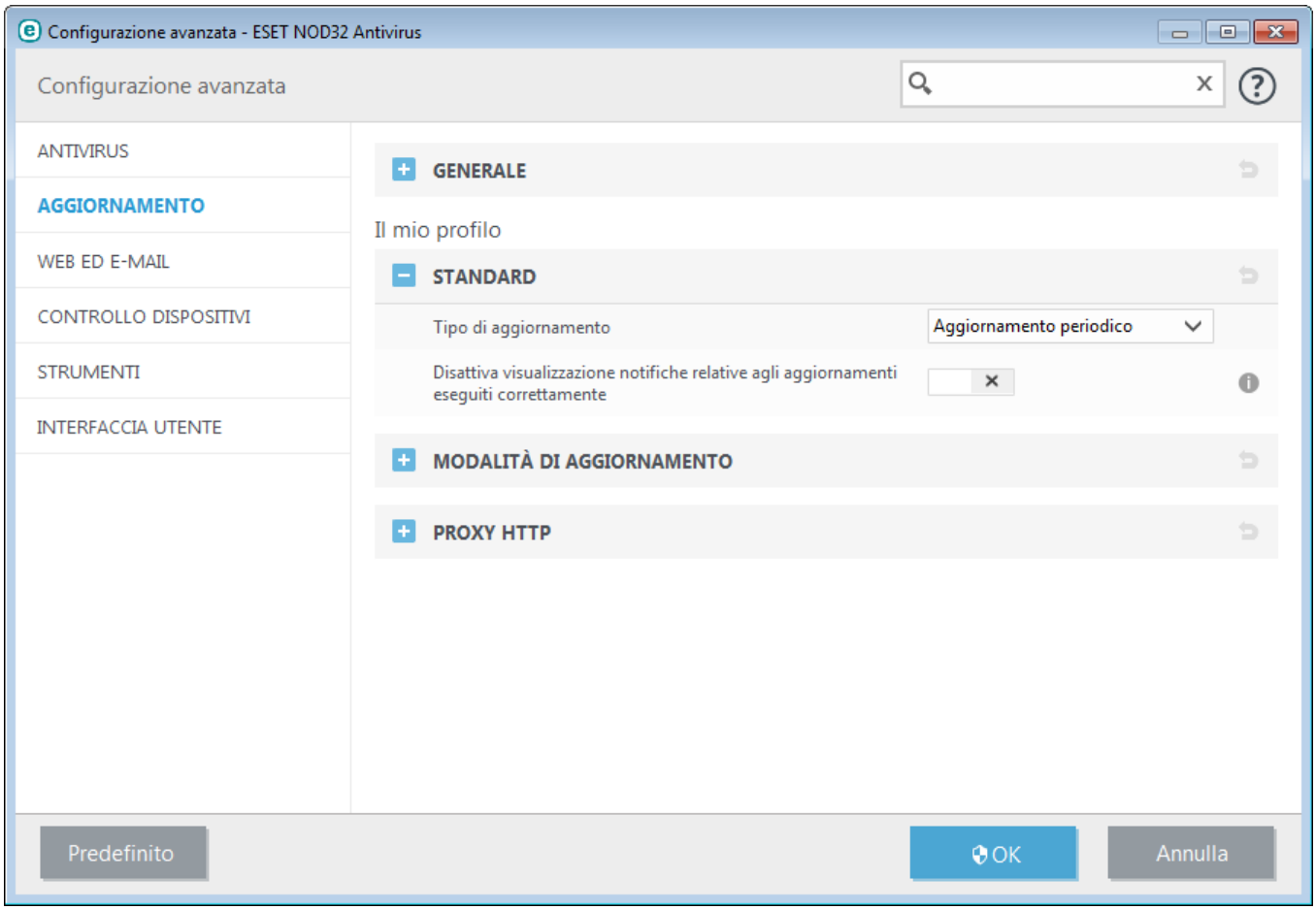
In caso di problemi durante il download degli aggiornamenti del database delle firme antivirali, fare clic su **Cancella** per eliminare i file/la cache di aggiornamento temporanei.

Annullamento

Se si sospetta che un nuovo aggiornamento del database delle firme antivirali e/o dei moduli del programma possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disattivare gli aggiornamenti per un determinato periodo di tempo. In alternativa, è possibile attivare gli aggiornamenti precedentemente disattivati nel caso in cui l'utente li abbia rimandati in maniera indefinita.

ESET NOD32 Antivirus registra gli snapshot del database delle firme antivirali e dei moduli del programma da utilizzare con la funzione *annullamento*. Per creare snapshot del database delle firme antivirali, lasciare selezionato il pulsante **Crea snapshot dei file di aggiornamento**. Il campo **Numero di snapshot memorizzati localmente** definisce il numero di snapshot del database delle firme antivirali precedentemente archiviati.

Se si fa clic su **Rollback** (**Configurazione avanzata** (F5) > **Aggiorna** > **Generale**), è necessario scegliere un intervallo temporale dal menu a discesa che indica il periodo di tempo nel quale gli aggiornamenti del database delle firme antivirali e del modulo di programma verranno sospesi.



Per scaricare correttamente gli aggiornamenti, occorre inserire tutti i parametri di aggiornamento richiesti. Se si utilizza un firewall, assicurarsi che al programma ESET sia consentito di comunicare con Internet (ad esempio, comunicazione HTTP).

Di base

Per impostazione predefinita, il **Tipo di aggiornamento** è impostato su **Aggiornamento periodico** per garantire che i file di aggiornamento vengano scaricati automaticamente dal server ESET che presenta il traffico di rete minore. Gli aggiornamenti pre-rilascio (opzione **Aggiornamento pre-rilascio**) sono aggiornamenti sottoposti ad approfondite verifiche interne che saranno presto disponibili per tutti. Gli aggiornamenti pre-rilascio consentono di accedere ai metodi di rilevamento e correzioni più recenti. È tuttavia probabile che tali aggiornamenti non siano sempre sufficientemente stabili e NON devono pertanto essere utilizzati su server di produzione e workstation dove è richiesta massima disponibilità e stabilità.

Disattiva visualizzazione notifiche relative agli aggiornamenti eseguiti correttamente: disattiva la notifica sulla barra delle applicazioni nell'angolo in basso a destra della schermata. È utile selezionare questa opzione se è in esecuzione un'applicazione a schermo intero o un videogioco. Tenere presente che la modalità presentazione disattiverà tutte le notifiche.

4.3.1.1 Aggiorna profili

Per varie configurazioni e attività di aggiornamento è possibile creare profili di aggiornamento. La creazione dei profili di aggiornamento è particolarmente utile per gli utenti mobili che necessitano di un profilo alternativo per le proprietà di connessione a Internet, soggette a periodici cambiamenti.

Nel menu a discesa **Profilo selezionato** è possibile visualizzare il profilo correntemente selezionato, configurato per impostazione predefinita come **Profilo personale**. Per creare un nuovo profilo, fare clic su **Profili...**, quindi su **Aggiungi...** e inserire il **Nome profilo**. Quando si crea un nuovo profilo, è possibile copiare le impostazioni da uno esistente selezionandolo dal menu a discesa **Copia impostazioni dal profilo**.

4.3.1.2 Impostazione aggiornamento avanzata

Per visualizzare la Configurazione aggiornamento avanzata, fare clic su **Configurazione...**. Le opzioni relative alla configurazione aggiornamento avanzata includono la configurazione della **Modalità di aggiornamento**, del **Proxy HTTP** e della **LAN**.

4.3.1.2.1 Modalità di aggiornamento

La scheda **Modalità di aggiornamento** contiene opzioni correlate all'aggiornamento dei componenti di programma. Il programma consente di preimpostare le azioni da eseguire quando è disponibile un nuovo aggiornamento dei componenti di programma.

Gli aggiornamenti dei componenti di programma aggiungono nuove funzioni o introducono modifiche alle funzioni già esistenti nelle versioni precedenti. Una volta installato l'aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer.

Aggiornamento applicazione: se attivata, l'aggiornamento di ciascun componente del programma sarà eseguito automaticamente e in modo silenzioso senza eseguire l'aggiornamento completo del prodotto.

Se è attiva l'opzione **Chiedi prima di scaricare l'aggiornamento**, verrà visualizzata una notifica ogni volta che è disponibile un nuovo aggiornamento.

Se la dimensione del file di aggiornamento supera il valore specificato nel campo **Chiedi se un file di aggiornamento è maggiore di (KB)**, verrà visualizzata una notifica.

4.3.1.2.2 Proxy HTTP

Per accedere alle opzioni di configurazione del server proxy per uno specifico profilo di aggiornamento, fare clic su **Aggiorna** nella struttura **Configurazione avanzata** (F5), quindi su **Proxy HTTP**. Fare clic sul menu a discesa **Modalità proxy** e selezionare una delle tre seguenti opzioni:

- Non utilizzare server proxy
- Connessione tramite server proxy
- Utilizza impostazioni server proxy globali

Se si seleziona l'opzione **Utilizza impostazioni server proxy globali**, verranno utilizzate le opzioni di configurazione del server proxy già specificate all'interno della sottostruttura **Strumenti** > **Server proxy** della struttura Configurazione avanzata.

Selezionare **Non utilizzare server proxy** per specificare che non verrà utilizzato alcun server proxy per l'aggiornamento di ESET NOD32 Antivirus.

Selezionare l'opzione **Connessione tramite server proxy** nei seguenti casi:

- È necessario utilizzare un server proxy per aggiornare ESET NOD32 Antivirus e tale server proxy è differente da quello specificato nelle impostazioni globali (**Strumenti** > **Server proxy**). In questo caso, sarà necessario fornire alcune informazioni aggiuntive: Indirizzo del **Server proxy**, **Porta** di comunicazione (3128 per impostazione predefinita), più **Nome utente** e **Password** per il server del proxy, se necessario.
- Le impostazioni del server proxy non sono state impostate a livello globale. ESET NOD32 Antivirus si connetterà tuttavia a un server proxy per verificare la disponibilità di aggiornamenti.
- Il computer è connesso a Internet tramite un server proxy. Le impostazioni vengono estrapolate da Internet Explorer durante l'installazione del programma, ma se successivamente vengono modificate, ad esempio se si cambia il provider di servizi Internet (ISP), verificare che le impostazioni del proxy HTTP elencate in questa finestra siano corrette. In caso contrario, il programma non sarà in grado di connettersi ai server di aggiornamento.

L'impostazione predefinita per il server proxy è **Utilizza impostazioni server proxy globali**.

NOTA: i dati di autenticazione, come ad esempio il **Nome utente** e la **Password**, sono necessari per accedere al server proxy. Compilare questi campi solo se sono richiesti un nome utente e una password. Tenere presente che questi campi, in cui non è necessario inserire il Nome utente e la Password per ESET NOD32 Antivirus, devono essere completati solo se è richiesta una password di accesso a Internet mediante un server proxy.

4.3.1.2.3 Connetti a LAN come

Durante l'aggiornamento da un server locale con una versione del sistema operativo Windows NT, per impostazione predefinita è richiesta l'autenticazione per ciascuna connessione di rete.

Per configurare un account simile, selezionare dal menu a discesa **Tipo di utente locale**:

- **Account di sistema (predefinito)**,
- **Utente corrente**,
- **Utente specificato**.

Selezionare **Account di sistema (predefinito)** per utilizzare l'account di sistema per l'autenticazione. In genere non viene eseguito alcun processo di autenticazione se nella sezione principale di impostazione dell'aggiornamento non sono specificati dati di autenticazione.

Per essere certi che il programma esegua l'autenticazione utilizzando l'account di un utente che ha eseguito correntemente l'accesso, selezionare **Utente attuale**. Lo svantaggio di questa soluzione consiste nel fatto che il programma non è in grado di connettersi al server di aggiornamento se nessun utente ha eseguito l'accesso in quel momento.

Selezionare **Utente specificato** se si desidera che il programma utilizzi un account utente specifico per l'autenticazione. Utilizzare questo metodo quando la connessione con l'account di sistema predefinito non riesce. Tenere presente che l'account dell'utente specificato deve disporre dell'accesso alla directory dei file di aggiornamento sul server locale. In caso contrario, il programma non sarà in grado di stabilire una connessione e scaricare gli aggiornamenti.

Avviso: Se si seleziona **Utente attuale** o **Utente specificato**, è possibile che si verifichi un errore quando si modifica l'identità del programma per l'utente desiderato. È consigliabile immettere i dati di autenticazione della LAN nella sezione principale di configurazione dell'aggiornamento. In questa sezione di impostazione dell'aggiornamento, i dati di autenticazione devono essere inseriti come segue: *nome_dominio**utente* (se si tratta di un gruppo di lavoro, immettere *none_gruppodilavoro**nome*) e la password utente. Per l'aggiornamento dalla versione HTTP del server locale, non è richiesta alcuna autenticazione.

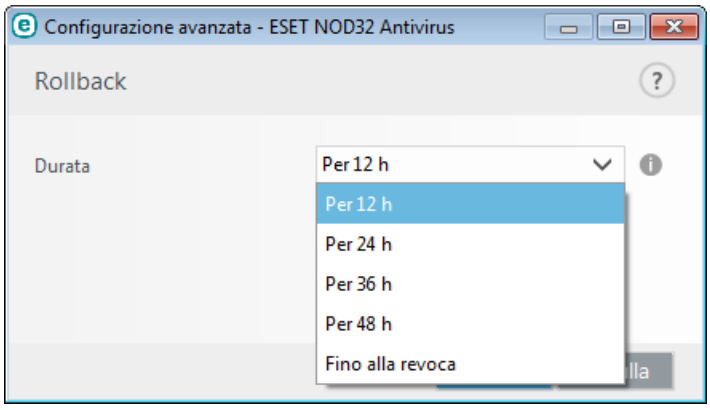
Attivare **Disconnetti dal server dopo l'aggiornamento** per forzare una disconnessione se una connessione al server dovesse rimanere attiva anche dopo il download degli aggiornamenti.

4.3.2 Rollback aggiornamento

Se si sospetta che un nuovo aggiornamento del database antivirus e/o dei moduli del programma possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disattivare gli aggiornamenti per un determinato periodo di tempo. In alternativa, è possibile attivare gli aggiornamenti precedentemente disattivati in caso di rimando indefinito da parte dell'utente.

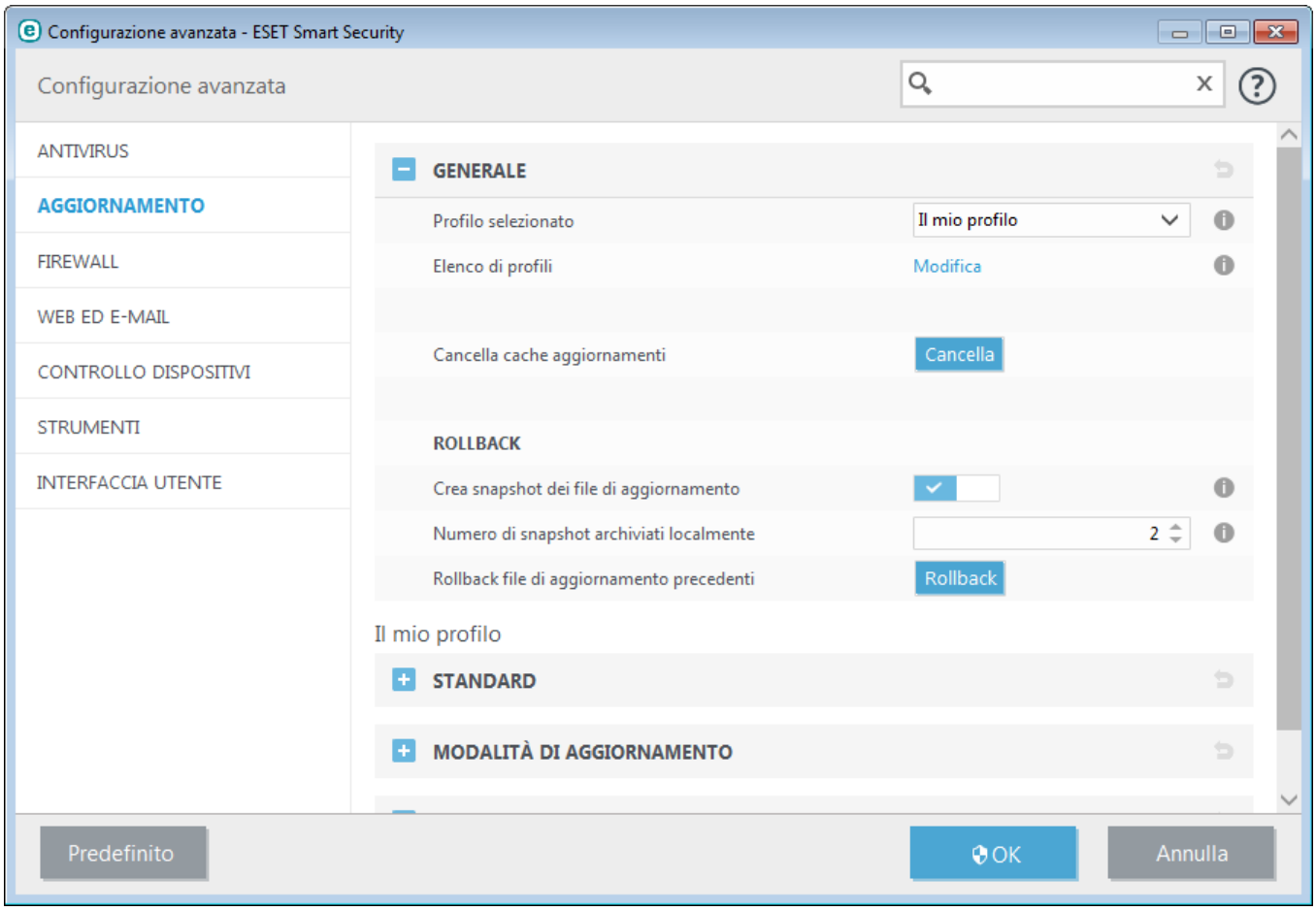
ESET NOD32 Antivirus registra gli snapshot del database delle firme antivirali e dei moduli del programma da utilizzare con la funzione *annullamento*. Per creare snapshot del database antivirus, lasciare selezionata la casella di controllo **Crea snapshot dei file di aggiornamento**. Il campo **Numero di snapshot memorizzati localmente** definisce il numero di snapshot del database antivirale precedentemente archiviati.

Dopo aver selezionato **Roll back** (**Configurazione avanzata** (F5) > **Aggiornamento** > **Rollback aggiornamento**), è necessario scegliere un intervallo di tempo nel menu a discesa **Sospendi aggiornamenti** che indica il periodo di tempo nel quale gli aggiornamenti del database delle firme antivirali e del modulo del programma verranno sospesi.



Selezionare **Fino a revoca** per rimandare in modo indefinito gli aggiornamenti periodici finché l'utente non avrà ripristinato la funzionalità degli aggiornamenti manualmente. Non è consigliabile selezionare questa opzione in quanto rappresenta un potenziale rischio per la protezione.

Se viene eseguito un rollback, il pulsante **Annulla** si trasforma in **Consenti aggiornamenti**. Non saranno consentiti aggiornamenti per l'intervallo di tempo selezionato nel menu a discesa **Sospendi aggiornamenti**. La versione del database delle firme antivirali viene ripristinata alla versione più vecchia a disposizione e memorizzata come uno snapshot nel file system del computer locale.



Esempio: Si presupponga che la versione più recente del database delle firme antivirali corrisponda al numero 6871. Le versioni 6870 e 6868 sono memorizzate come snapshot del database delle firme antivirali. Si noti che la versione 6869 non è disponibile poiché, ad esempio, il computer è stato spento ed è stato reso disponibile un aggiornamento più recente prima che venisse scaricata la versione 6869. Se il campo **Numero di snapshot memorizzati localmente** è impostato su 2 e si fa clic su **Annulla**, il database delle firme antivirali (compresi i moduli del programma) viene ripristinato al numero di versione 6868. L'operazione potrebbe richiedere alcuni minuti. Verificare se la versione del database delle firme antivirali è stata ripristinata a una versione precedente dalla finestra principale del programma di ESET NOD32 Antivirus nella sezione Aggiornamento.

4.3.3 Come creare attività di aggiornamento

È possibile avviare gli aggiornamenti manualmente selezionando l'opzione **Aggiorna database delle firme antivirali** nella finestra principale visualizzata dopo aver selezionato l'opzione **Aggiorna** dal menu principale.

Gli aggiornamenti possono essere eseguiti anche come attività programmate. Per configurare un'attività programmata, fare clic su **Strumenti** > **Pianificazione attività**. Per impostazione predefinita, in ESET NOD32 Antivirus sono attivate le seguenti attività:

- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna delle attività di aggiornamento in base alle proprie esigenze. Oltre alle attività di aggiornamento predefinite, è possibile creare nuove attività di aggiornamento con una configurazione definita dall'utente. Per ulteriori dettagli sulla creazione e sulla configurazione delle attività di aggiornamento, consultare la sezione Pianificazione attività.

4.4 Strumenti

Il menu **Strumenti** include moduli che consentono di semplificare l'amministrazione del programma, offrendo opzioni aggiuntive per gli utenti esperti.

4.4.1 Strumenti in ESET NOD32 Antivirus

Il menu **Strumenti** include moduli che consentono di semplificare l'amministrazione del programma, offrendo opzioni aggiuntive per gli utenti esperti.

Questo menu contiene i seguenti strumenti:

File di rapporto

Statistiche di protezione

Attività di verifica

Processi in esecuzione (se ThreatSense è attivato in ESET NOD32 Antivirus)

ESET SysInspector

ESET SysRescue: reindirizza l'utente alla pagina Live di ESET SysRescue, dove è possibile scaricare l'immagine Live di ESET SysRescue o il Live CD/USB Creator per i sistemi operativi Microsoft Windows.

Pianificazione attività

Invia campione per analisi: consente all'utente di inviare un file sospetto al laboratorio di ricerca ESET per l'analisi. La finestra di dialogo visualizzata dopo aver selezionato questa opzione è descritta in questa sezione.

Quarantena

NOTA: ESET SysRescue potrebbe non essere disponibile per Windows 8 in versioni precedenti di prodotti di protezione ESET. In questo caso, si consiglia di effettuare l'upgrade del prodotto o di creare un disco ESET SysRescue su un'altra versione di Microsoft Windows.

4.4.1.1 File di rapporto

I file di rapporto contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. La registrazione rappresenta una parte essenziale dell'analisi del sistema, del rilevamento delle minacce e della risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento da parte dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di rapporto correnti. È possibile visualizzare i messaggi di testo e i rapporti direttamente dall'ambiente di ESET NOD32 Antivirus, nonché dai registri di archivio.

È possibile accedere ai file di rapporto dalla finestra principale del programma facendo clic su **Strumenti** > **File di rapporto**. Selezionare il tipo di rapporto desiderato nel menu a discesa **Rapporto**. Sono disponibili i rapporti seguenti:

- **Minacce rilevate** - Nel rapporto delle minacce sono contenute informazioni dettagliate sulle infiltrazioni rilevate da ESET NOD32 Antivirus. Le informazioni contenute nel rapporto includono l'ora del rilevamento, il nome dell'infiltrazione, la posizione, l'azione eseguita e il nome dell'utente registrato nel momento in cui è stata rilevata l'infiltrazione. Fare doppio clic su una voce qualsiasi del rapporto per visualizzarne il contenuto dettagliato in una finestra separata.
- **Eventi** - Tutte le azioni importanti eseguite da ESET NOD32 Antivirus vengono registrate nel rapporto eventi. Il rapporto eventi contiene informazioni sugli eventi e sugli errori che si sono verificati nel programma. È utile agli amministratori di sistema e agli utenti per risolvere i problemi. Spesso le informazioni visualizzate in questo rapporto consentono di trovare la soluzione a un problema che si verifica nel programma.
- **Controllo computer** - In questa finestra vengono visualizzati i risultati di tutti i controlli manuali o pianificati completati. Ogni riga corrisponde a un singolo controllo del computer. Fare doppio clic su una voce per visualizzare i dettagli del rispettivo controllo.
- **HIPS**: contiene i record di specifiche regole HIPS che sono contrassegnati per la registrazione. Nel protocollo viene mostrata l'applicazione che ha attivato l'operazione, il risultato (ovvero se la regola era consentita o vietata) e il nome della regola creata.
- **Siti Web filtrati** - Questo elenco è utile se si desidera visualizzare un elenco di siti Web che sono stati bloccati dalla Protezione accesso Web. In questi rapporti è possibile visualizzare l'ora, l'indirizzo URL, l'utente e l'applicazione che hanno creato una connessione a un sito Web specifico.

- **Controllo dispositivi** - Contiene record relativi ai supporti rimovibili o ai dispositivi collegati al computer. Nel file di rapporto saranno registrati solo i dispositivi con le rispettive regole di Controllo dispositivi. Se la regola non corrisponde a un dispositivo collegato, non verrà creata alcuna voce di rapporto relativa a tale evento. Qui è possibile visualizzare anche dettagli relativi al tipo di dispositivo, numero di serie, nome del fornitore e dimensioni del supporto (ove disponibili).

In ciascuna sezione, le informazioni visualizzate possono essere copiate negli Appunti selezionando la voce desiderata e utilizzando il tasto di scelta rapida **Ctrl + C**. Per selezionare più voci, utilizzare i tasti **Ctrl** e **Maiusc**.

Fare clic su **Filtraggio** per aprire la finestra **Filtraggio rapporti** in cui è possibile definire i criteri di filtraggio.

Fare clic con il pulsante destro del mouse su un record specifico per visualizzare il menu contestuale. Nel menu contestuale sono disponibili le seguenti opzioni:

- **Mostra:** consente di visualizzare informazioni più dettagliate relative al rapporto selezionato in una nuova finestra.
- **Filtra gli stessi record**: dopo aver attivato questo filtro, verranno visualizzati esclusivamente i record dello stesso tipo (diagnostica, avvisi, ecc.).
- **Filtro.../Trova...**: dopo aver selezionato questa opzione, la finestra Cerca nel rapporto consentirà all'utente di definire i criteri di filtraggio per voci specifiche dei rapporti.
- **Attiva filtro**: attiva le impostazioni del filtro.
- **Disattiva filtro**: consente di annullare tutte le impostazioni del filtro (come descritto in precedenza).
- **Copia/Copia tutto**: copia le informazioni su tutti i record nella finestra.
- **Elimina/Elimina tutto** - Elimina i record selezionati o tutti i record visualizzati. Per poter eseguire questa operazione è necessario disporre dei privilegi amministrativi.
- **Esporta...**: esporta le informazioni sul/i record in formato XML.
- **Esporta tutto...**: esporta le informazioni sui record in formato XML.
- **Scorri registro**: lasciare attivata questa opzione per scorrere automaticamente i rapporti meno recenti e visualizzare i rapporti attivi nella finestra **File di rapporto**.

4.4.1.1.1 File di rapporto

La configurazione della registrazione di ESET NOD32 Antivirus è accessibile dalla finestra principale del programma. Fare clic su **Configurazione** > **Accedi a configurazione avanzata...** > **Strumenti** > **File di rapporto**. La sezione relativa ai rapporti viene utilizzata per definire come verranno gestiti. Il programma elimina automaticamente i rapporti meno recenti per liberare spazio sull'unità disco rigido. Per i file di rapporto è possibile specificare le opzioni seguenti:

Livello di dettaglio di registrazione minimo - Specifica il livello di dettaglio minimo degli eventi da registrare.

- **Diagnostica** - Registra tutte le informazioni necessarie per l'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativi** - Messaggi di record informativi che includono gli aggiornamenti riusciti e tutti i record indicati in precedenza.
- **Allarmi** - Consente di registrare errori critici e messaggi di allarme.
- **Errori** - Verranno registrati errori quali *"Errore durante il download del file"* ed errori critici.
- **Critici** - Registra solo gli errori critici (errore che avvia la protezione antiviruse così via).

Le voci del rapporto più vecchie del numero specificato di giorni nel campo **Elimina automaticamente i record più vecchi di (giorni)** verranno eliminate automaticamente.

Ottimizza automaticamente file di rapporto - Se questa opzione è selezionata, i file di rapporto vengono automaticamente deframmentati se la percentuale è superiore al valore specificato nel campo **Se il numero di record inutilizzati supera (%)**.

Fare clic su **Ottimizza** per avviare la deframmentazione dei file di rapporto. Per migliorare le prestazioni e potenziare la velocità di elaborazione dei rapporti, durante questo processo vengono rimosse le voci vuote. Tale miglioramento può essere rilevato in particolare se i rapporti contengono un numero elevato di elementi.

Attiva protocollo di testo consente di attivare l'archiviazione dei rapporti in un altro formato di file separato da File di rapporto:

- **Directory di destinazione**: directory in cui verranno archiviati i file di rapporto (si applica solo ai file di testo/CSV). Ciascuna sezione del rapporto presenta il proprio file con un nome predefinito (ad esempio, *virlog.txt* per la sezione **Minacce rilevate** dei file di rapporto, se si utilizza un formato di file testo normale per l'archiviazione dei rapporti).
- **Tipo**: selezionando il formato di file **Testo**, i rapporti verranno archiviati in un file di testo e i dati saranno suddivisi in schede. Le stesse condizioni si applicano al formato di file **CSV** separato da virgole. Se si sceglie **Evento**, i rapporti verranno archiviati nel rapporto eventi Windows (che è possibile visualizzare utilizzando il visualizzatore eventi nel Pannello di controllo) anziché nel file.

Elimina tutti i file del rapporto: elimina tutti i rapporti attualmente archiviati selezionati nel menu a discesa **Tipo**. Verrà visualizzata una notifica relativa all'avvenuta eliminazione dei rapporti.

NOTA: per una più rapida risoluzione dei problemi, ESET potrebbe richiedere all'utente di fornire i rapporti archiviati sul computer. ESET Log Collector facilita la raccolta delle informazioni necessarie. Per ulteriori informazioni su ESET Log Collector, consultare l'articolo della Knowledge Base ESET.

4.4.1.1.2 Microsoft NAP

La NAP (Network Access Protection) è una tecnologia Microsoft per il controllo dell'accesso di rete di un computer host basato sull'integrità del sistema host, che consente agli amministratori di sistema di una rete di computer di un'organizzazione di definire i criteri per i requisiti di integrità del sistema.

La Network Access Protection (NAP) è stata concepita allo scopo di aiutare gli amministratori a preservare lo stato di integrità dei computer presenti nella rete che, a sua volta, contribuisce al mantenimento dell'integrità complessiva della rete. Lo strumento non consente di proteggere una rete da utenti con scopi illegittimi. Ad esempio, se su un computer sono presenti tutti i software e le configurazioni richiesti dai criteri di accesso alla rete, il sistema viene considerato integro o conforme e potrà accedere adeguatamente alla rete. La NAP non impedisce a un utente autorizzato con un computer conforme di caricare un programma dannoso sulla rete o di adottare un altro comportamento inappropriato,

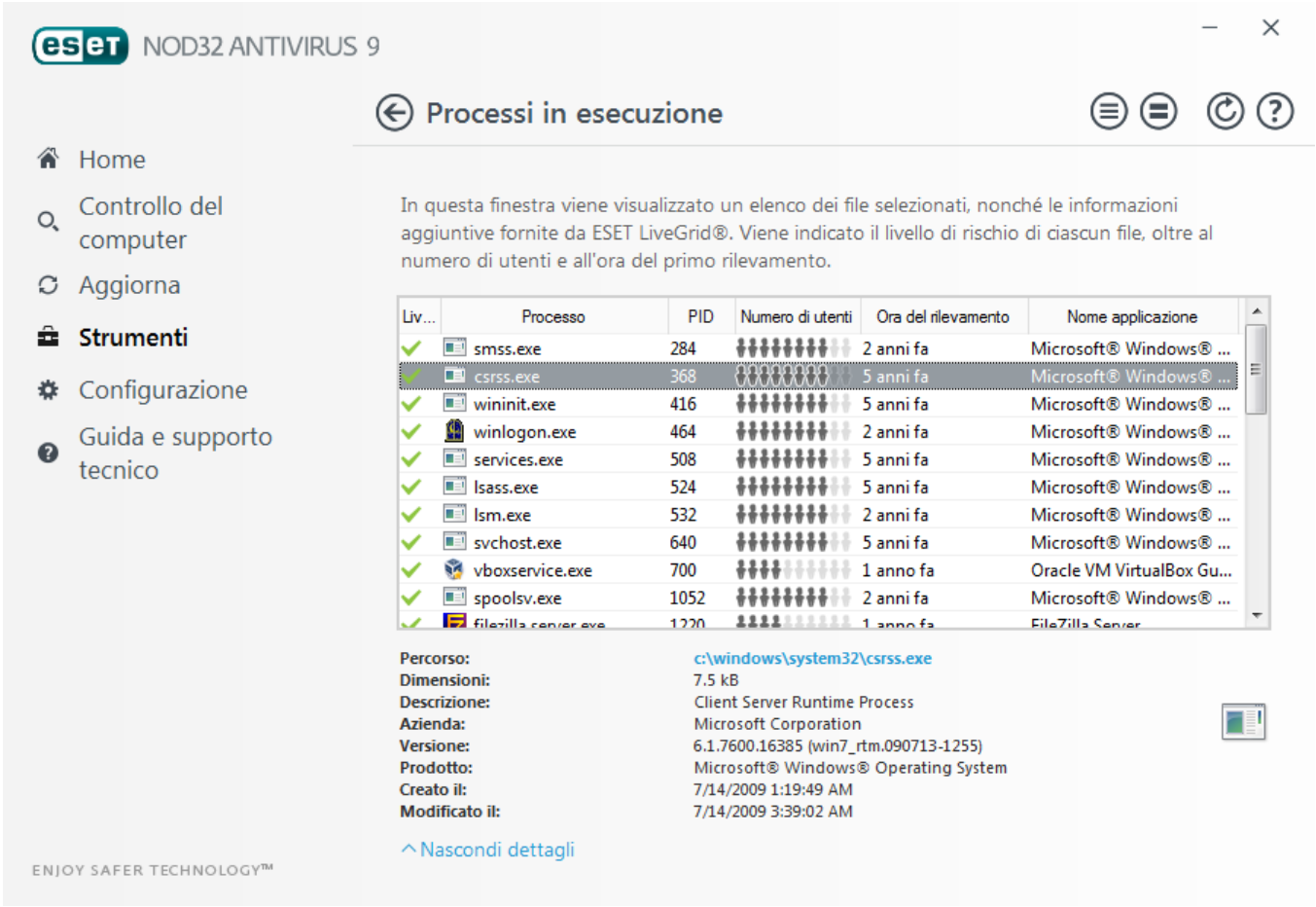
ma consente agli amministratori di creare e attuare criteri di integrità per i computer che si connettono alla rete aziendale. I criteri disciplinano sia i componenti software installati sia le configurazioni di sistema. I computer connessi alla rete, come computer portatili, workstation e altri dispositivi simili, vengono valutati in base ai requisiti di integrità configurati.

I requisiti di integrità includono:

• È stato attivato un firewall.
• È stato installato un programma antivirus.
• Il programma antivirus è aggiornato.
• Sono stati attivati gli aggiornamenti automatici di Windows e così via.

4.4.1.2 Processi in esecuzione

I processi in esecuzione consentono di visualizzare i programmi o processi in esecuzione sul computer e inviare informazioni tempestive e costanti a ESET sulle nuove infiltrazioni. ESET NOD32 Antivirus fornisce informazioni dettagliate sui processi in esecuzione allo scopo di proteggere gli utenti che utilizzano la tecnologia ThreatSense.


NOD32 ANTIVIRUS 9
Processi in esecuzione
Home
Controllo del computer
Aggiorna
Strumenti
Configurazione
Guida e supporto tecnico
In questa finestra viene visualizzato un elenco dei file selezionati, nonché le informazioni aggiuntive fornite da ESET LiveGrid®. Viene indicato il livello di rischio di ciascun file, oltre al numero di utenti e all'ora del primo rilevamento.
Liv... Processo PID Numero di utenti Ora del rilevamento Nome applicazione
smss.exe 284 2 anni fa Microsoft® Windows® ...
csrss.exe 368 5 anni fa Microsoft® Windows® ...
wininit.exe 416 5 anni fa Microsoft® Windows® ...
winlogon.exe 464 2 anni fa Microsoft® Windows® ...
services.exe 508 5 anni fa Microsoft® Windows® ...
lsass.exe 524 5 anni fa Microsoft® Windows® ...
lsm.exe 532 2 anni fa Microsoft® Windows® ...
svchost.exe 640 5 anni fa Microsoft® Windows® ...
vboxservice.exe 700 1 anno fa Oracle VM VirtualBox Gu...
spoolsv.exe 1052 2 anni fa Microsoft® Windows® ...
Percorso: c:\windows\system32\csrss.exe
Dimensioni: 7.5 kB
Descrizione: Client Server Runtime Process
Azienda: Microsoft Corporation
Versione: 6.1.7600.16385 (win7_rtm.090713-1255)
Prodotto: Microsoft® Windows® Operating System
Creato il: 7/14/2009 1:19:49 AM
Modificato il: 7/14/2009 3:39:02 AM
Nascondi dettagli
ENJOY SAFER TECHNOLOGY™

Processo - Nome immagine del programma o del processo attualmente in esecuzione sul computer. Per visualizzare tutti i processi in esecuzione sul computer è inoltre possibile utilizzare Windows Task Manager. Per aprire il Task Manager, fare clic con il pulsante destro del mouse su un'area vuota sulla barra delle attività, quindi scegliere **Task Manager** oppure premere Ctrl+Maiusc+Esc sulla tastiera.

Livello rischio - Nella maggior parte dei casi, ESET NOD32 Antivirus e la tecnologia ThreatSense assegnano livelli di rischio agli oggetti (file, processi, chiavi di registro, ecc.), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ogni oggetto e quindi ne valutano le potenzialità come attività dannosa. Sulla base di tali euristiche, agli oggetti viene assegnato un livello di rischio da 1 - Non a rischio (verde) a 9 - A rischio (rosso).

NOTA: Le applicazioni note contrassegnate come Non a rischio (verde) sono definitivamente pulite (inserite nella whitelist) e saranno escluse dal controllo in modo da aumentare la velocità di esecuzione del controllo del computer su richiesta o della protezione file system in tempo reale sul dispositivo.

Numero di utenti - Numero di utenti che utilizzano una determinata applicazione. Queste informazioni sono raccolte mediante la tecnologia ThreatSense.

Ora di rilevamento - Periodo di tempo da quando l'applicazione è stata rilevata dalla tecnologia ThreatSense.

NOTA: se un'applicazione è contrassegnata con un livello di rischio Sconosciuto (arancione), non si tratta necessariamente di software dannoso. In genere si tratta di una nuova applicazione. In caso di dubbi sul file, selezionare l'opzione invia file per analisi al laboratorio di ricerca ESET. Se il file si rivela essere un'applicazione dannosa, il suo rilevamento verrà aggiunto in uno degli aggiornamenti successivi.

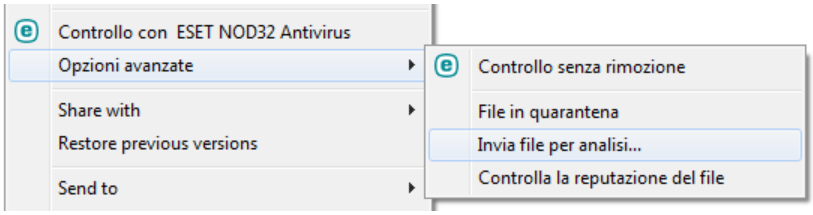
Nome applicazione - Nome specifico di un programma o processo.

Apri una nuova finestra - Le informazioni sui processi in esecuzione verranno visualizzate in una nuova finestra.

Fare clic sulla parte inferiore di una determinata applicazione per visualizzare le seguenti informazioni nella parte inferiore della finestra:

- **File** - Posizione di un'applicazione sul computer.
- **Dimensioni file** - Dimensione del file in B (byte).
- **Descrizione file** - Caratteristiche del file basate sulla relativa descrizione del sistema operativo.
- **Nome società** - Nome del fornitore o del processo applicativo.
- **Versione file** - Informazioni estrapolate dall'autore dell'applicazione.
- **Nome prodotto** - Nome dell'applicazione e/o nome commerciale.

NOTA: La reputazione può essere controllata anche sui file che non agiscono come programmi/processi in esecuzione - contrassegnare i file che si desidera controllare, fare clic con il pulsante destro del mouse su di essi e selezionare **Opzioni avanzate** > **Controlla la reputazione del file tramite ThreatSense**.



4.4.1.3 Statistiche di protezione

Per visualizzare un grafico dei dati statistici relativi ai moduli di protezione ESET NOD32 Antivirus, fare clic su **Strumenti** > **Statistiche di protezione**. Selezionare il modulo di protezione desiderato dal menu a discesa **Statistiche** per visualizzare il grafico e la legenda corrispondenti. Se si passa il mouse su un elemento nella legenda, verranno visualizzati solo i dati di quell'elemento nel grafico.

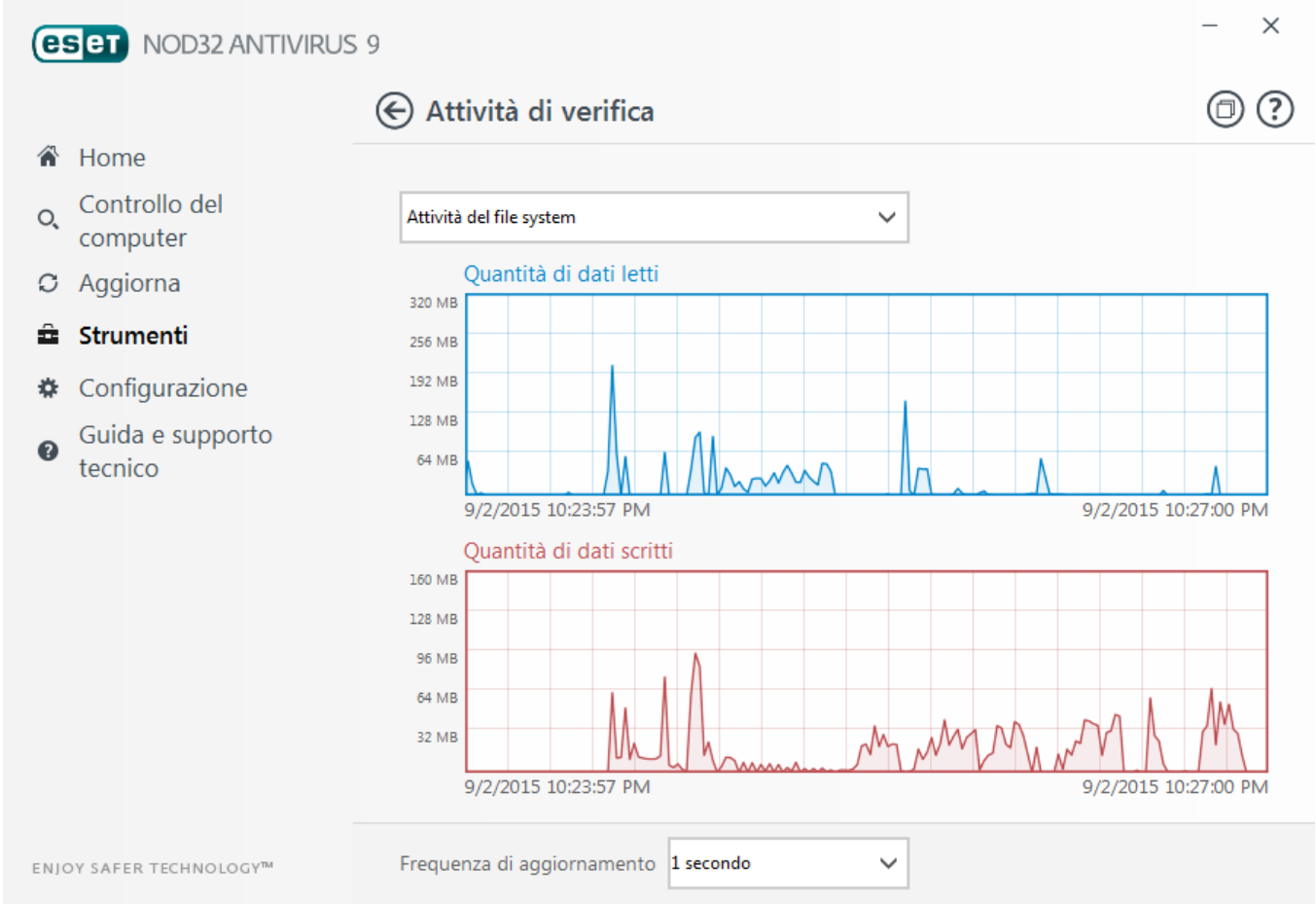
Sono disponibili i seguenti grafici statistici:

- **Protezione antivirus e antispyware** - Consente di visualizzare il numero di oggetti infetti e puliti.
- **Protezione file system** - Consente di visualizzare solo gli oggetti che sono stati scritti o letti sul file system.
- **Protezione client e-mail** - Consente di visualizzare solo gli oggetti inviati o ricevuti dai client e-mail.
- **Protezione accesso Web e Anti-Phishing** - Consente di visualizzare solo gli oggetti scaricati dai browser Web.

Sotto il grafico delle statistiche è visualizzato il numero degli oggetti totali sottoposti a controllo, l'ultimo oggetto sottoposto a controllo e la data e l'ora delle statistiche. Fare clic su **Azzeramento** per cancellare tutte le informazioni statistiche.

4.4.1.4 Attività di verifica

Per visualizzare l'**Attività di file system** corrente in un grafico, fare clic su **Strumenti** > **Attività di verifica**. Nella parte inferiore del grafico è presente una linea cronologica che registra in tempo reale le attività del file system in base all'intervallo di tempo selezionato. Per modificare l'intervallo di tempo, selezionarlo nel menu a discesa **Frequenza di aggiornamento**.



Sono disponibili le seguenti opzioni:

- **Passaggio: 1 secondo**: il grafico si aggiorna ogni secondo e l'intervallo di tempo copre gli ultimi 10 minuti.
- **Passaggio: 1 minuto (ultime 24 ore)**: il grafico si aggiorna ogni minuto e l'intervallo di tempo copre le ultime 24 ore.
- **Passaggio: 1 ora (ultimo mese)**: il grafico si aggiorna ogni ora e l'intervallo di tempo copre l'ultimo mese.
- **Passaggio: 1 ora (mese selezionato)**: il grafico si aggiorna ogni ora e l'intervallo di tempo copre gli ultimi X mesi selezionati.

L'asse verticale del **Grafico dell'attività del file system** rappresenta i dati letti (blu) e scritti (rosso). Entrambi i valori sono espressi in KB (kilobyte)/MB/GB. Facendo scorrere il mouse sui dati letti o scritti nella didascalia sottostante il grafico, è possibile visualizzare unicamente i dati relativi a quella specifica attività.

4.4.1.5 ESET SysInspector

ESET SysInspector è un'applicazione che esamina a fondo il computer, raccoglie informazioni dettagliate sui componenti del sistema, quali driver e applicazioni, le connessioni di rete o le voci di registro importanti e valuta il livello di rischio di ciascun componente. Tali informazioni possono risultare utili per determinare la causa di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

Nella finestra di dialogo SysInspector sono visualizzate le seguenti informazioni sui rapporti creati:

- **Ora** - Ora di creazione del rapporto.
- **Commento** - Breve commento.
- **Utente** - Nome dell'utente che ha creato il rapporto.
- **Stato** - Stato di creazione del rapporto.

Sono disponibili le azioni seguenti:

- **Apri**: apre il rapporto creato. È inoltre possibile fare clic con il pulsante destro del mouse su uno specifico file di registro e selezionare **Mostra** dal menu contestuale.
- **Confronta** - Consente di mettere a confronto due rapporti esistenti.
- **Crea...** - Consente di creare un nuovo rapporto. Attendere fino al termine di ESET SysInspector (lo stato del rapporto comparirà come Creato) prima di provare ad accedere al rapporto.
- **Elimina**: rimuove dall'elenco il rapporto o i rapporti selezionati.

Le seguenti opzioni sono disponibili nel menu contestuale in caso di selezione di uno o più file di rapporto:

- **Mostra** - Visualizza il rapporto selezionato in ESET SysInspector (funzione uguale all'esecuzione di un doppio clic su un rapporto).
- **Confronta**: consente di mettere a confronto due rapporti esistenti.
- **Crea...**: consente di creare un nuovo rapporto. Attendere fino al termine di ESET SysInspector (lo stato del rapporto comparirà come Creato) prima di provare ad accedere al rapporto.
- **Elimina tutto** - Consente di eliminare tutti i rapporti.
- **Esporta...** - Esporta il rapporto su un file *XML* o su un file *XML* compresso.

4.4.1.6 Pianificazione attività

La Pianificazione attività consente di gestire e avviare attività pianificate con configurazione e proprietà predefinite.

È possibile accedere alla Pianificazione attività nella finestra principale del programma di ESET NOD32 Antivirus facendo clic su **Strumenti** > **Pianificazione attività**. La **Pianificazione attività** contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, ad esempio data, ora e profilo di controllo predefiniti utilizzati.

La Pianificazione attività consente di pianificare le attività seguenti: aggiornamento del database delle firme antivirali, attività di scansione, controllo dei file di avvio del sistema e manutenzione dei rapporti. È possibile aggiungere o modificare attività direttamente dalla finestra principale Pianificazione attività, facendo clic su **Aggiungi...** o **Elimina** nella parte inferiore della finestra. Fare clic con il pulsante destro del mouse in qualsiasi punto della finestra Pianificazione attività per eseguire le azioni seguenti: visualizzare informazioni dettagliate, eseguire immediatamente l'attività, aggiungere una nuova attività ed eliminare un'attività esistente. Utilizzare le caselle di controllo accanto a ciascuna voce per attivare o disattivare le attività.

Per impostazione predefinita, in **Pianificazione attività** vengono visualizzate le attività pianificate seguenti:

- **Manutenzione rapporto**
- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**
- **Controlla periodicamente la disponibilità di una versione del prodotto più recente** (vedere Modalità di aggiornamento)
- **Controllo automatico file di avvio** (dopo l'accesso utente)
- **Controllo automatico file di avvio** (dopo il completamento dell'aggiornamento del database delle firme antivirali)
- **Primo controllo automatico**

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), fare clic con il pulsante destro del mouse sull'attività e selezionare **Modifica...** oppure selezionare l'attività che si desidera modificare e fare clic su **Modifica...**.

Aggiunta di un nuova attività

1. Fare clic su **Aggiungi attività** nella parte inferiore della finestra.
2. Inserire il nome dell'attività.
3. Selezionare l'attività desiderata dal menu a discesa:

- **Esegui applicazione esterna**: consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto**: i file di rapporto contengono anche gli elementi rimasti dai record eliminati. Questa attività ottimizza periodicamente i record nei file di rapporto allo scopo di garantire un funzionamento efficiente.
- **Controllo del file di avvio del sistema**: consente di controllare i file la cui esecuzione è consentita all'avvio del sistema o all'accesso.
- **Crea un controllo computer**: crea uno snapshot ESET SysInspector del computer, raccoglie informazioni dettagliate sui componenti del sistema (ad esempio, driver e applicazioni) e valuta il livello di rischio di ciascun componente.
- **Controllo computer su richiesta**: consente di eseguire un controllo di file e di cartelle sul computer in uso.
- **Primo controllo**: per impostazione predefinita, 20 minuti dopo l'installazione o il riavvio, verrà eseguito un controllo del computer come attività con priorità bassa.
- **Aggiorna**: pianifica un'attività di aggiornamento aggiornando il database delle firme antivirali e i moduli del programma.

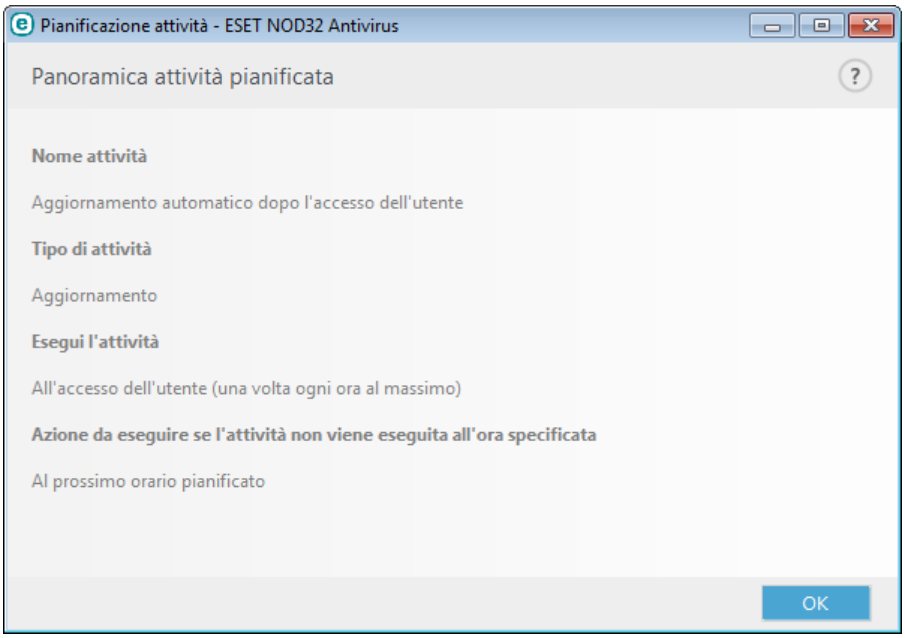
4. Premere il pulsante **Attivata** se si desidera attivare l'attività (è possibile eseguire questa operazione in un secondo momento selezionando/deselezionando la casella di controllo nell'elenco di attività pianificate), fare clic su **Avanti** e selezionare una delle opzioni relative alla frequenza di esecuzione:

- **Una volta** - L'attività verrà eseguita alla data e all'ora predefinite.
- **Ripetutamente** - L'attività verrà eseguita in base all'intervallo di tempo specificato.
- **Ogni giorno** - L'attività verrà eseguita periodicamente ogni giorno all'ora specificata.
- **Ogni settimana**: l'attività verrà eseguita nel giorno e all'ora selezionati.
- **Quando si verifica un evento** - L'attività verrà eseguita quando si verifica un evento specifico.

5. Selezionare **Ignora attività se in esecuzione su un computer alimentato dalla batteria** per ridurre al minimo le risorse di sistema in caso di utilizzo della batteria del computer portatile. L'attività verrà eseguita alla data e all'ora specificate nei campi **Esecuzione attività**. Se l'attività non è stata eseguita all'ora predefinita, è possibile specificare il momento in cui dovrà essere nuovamente eseguita:

- **Al prossimo orario pianificato**
- **Prima possibile**
- **Immediatamente, se l'ora dall'ultima esecuzione supera un valore specificato** (è possibile definire l'intervallo utilizzando la casella di scorrimento **Ora dall'ultima esecuzione**)

È possibile rivedere l'attività pianificata facendo clic con il pulsante tasto destro del mouse, quindi su **Mostra dettagli attività**.


Pianificazione attività - ESET NOD32 Antivirus
Panoramica attività pianificata
Nome attività
Aggiornamento automatico dopo l'accesso dell'utente
Tipo di attività
Aggiornamento
Esegui l'attività
All'accesso dell'utente (una volta ogni ora al massimo)
Azione da eseguire se l'attività non viene eseguita all'ora specificata
Al prossimo orario pianificato
OK

4.4.1.7 ESET SysRescue

ESET SysRescue è un'utilità che consente all'utente di creare un disco di avvio contenente una delle soluzioni ESET Security, tra cui ESET NOD32 Antivirus, ESET Smart Security o alcuni prodotti per server. Il vantaggio principale offerto da ESET SysRescue consiste nel fatto che la soluzione ESET Security viene eseguita indipendentemente dal sistema operativo che la ospita ma con un accesso diretto al disco e al file system. Ciò consente di rimuovere infiltrazioni che non sarebbe stato possibile eliminare in una situazione ordinaria, ad esempio durante l'esecuzione del sistema operativo.

4.4.1.8 ESET LiveGrid®

ESET LiveGrid® (sviluppato sul sistema avanzato di allarme immediato ESET ThreatSense.Net) utilizza i dati inviati dagli utenti ESET di tutto il mondo e li invia al laboratorio di ricerca ESET. Grazie all'invio di campioni e metadati "from the wild" sospetti, ESET LiveGrid® consente a ESET di soddisfare le esigenze dei clienti e di gestire le minacce più recenti in modo tempestivo. Per ulteriori informazioni su ESET LiveGrid®, consultare il glossario.

Un utente può controllare la reputazione dei processi in esecuzione e dei file direttamente dall'interfaccia del programma o dal menu contestuale. Ulteriori informazioni sono disponibili su ESET LiveGrid®. Sono disponibili due opzioni:

1. È possibile scegliere di non attivare ESET LiveGrid®. Non verrà persa alcuna funzionalità del software, ma, in alcuni casi, ESET NOD32 Antivirus potrebbe rispondere più rapidamente alle nuove minacce rispetto all'aggiornamento del database delle firme antivirali quando ESET Live Grid è attivato.
2. È possibile configurare ESET LiveGrid® per l'invio di informazioni anonime sulle nuove minacce e laddove sia presente il nuovo codice dannoso. Il file può essere inviato a ESET per un'analisi dettagliata. Lo studio di queste minacce sarà d'aiuto ad ESET per aggiornare le proprie capacità di rilevamento.

ESET LiveGrid® raccoglierà informazioni sul computer dell'utente in relazione alle nuove minacce rilevate. Tali informazioni possono includere un campione o una copia del file in cui è contenuta la minaccia, il percorso al file, il nome del file, informazioni su data e ora, il processo in base al quale la minaccia è apparsa sul computer e informazioni sul sistema operativo del computer.

Per impostazione predefinita, ESET NOD32 Antivirus viene configurato per l'invio di file sospetti al laboratorio antivirus ESET per l'analisi dettagliata. Sono sempre esclusi file con determinate estensioni, ad esempio *DOC* o *XLS*. È inoltre possibile aggiungere altre estensioni qualora sussistano specifici file che l'utente o la società dell'utente non desidera inviare.

Nel menu di configurazione ESET LiveGrid® sono disponibili varie opzioni di attivazione/disattivazione di ESET LiveGrid®, uno strumento utile per l'invio di file sospetti e di informazioni statistiche anonime ai laboratori ESET. È accessibile dalla struttura di Configurazione avanzata selezionando **Strumenti** > **ESET LiveGrid®**.

Attiva il sistema di reputazione ESET LiveGrid® (scelta consigliata) - Il sistema di reputazione ESET LiveGrid® potenzia le prestazioni delle soluzioni anti-malware ESET eseguendo un confronto tra i file controllati e un database di oggetti inseriti nelle whitelist o nelle blacklist all'interno del cloud.

Invia statistiche anonime: consente a ESET di raccogliere informazioni sulle nuove minacce rilevate, tra cui il nome della minaccia, la data e l'ora del rilevamento, il metodo di rilevamento e i metadati associati, la versione e la configurazione del prodotto, incluse le informazioni sul sistema in uso.

Invia file - I file sospetti simili alle minacce e/o i file con caratteristiche o comportamenti anomali vengono inviati a ESET ai fini dell'analisi.

Selezionare **Attiva registrazione** per creare un rapporto di eventi sul quale vengono registrati gli invii dei file e delle informazioni statistiche. Ciò attiverà la registrazione sul Rapporto eventi dell'invio di file o statistiche.

Contatto e-mail (facoltativo): il contatto e-mail può essere incluso insieme ai file sospetti e utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Tenere presente che non si riceverà alcuna risposta da ESET, a meno che non siano richieste ulteriori informazioni.

Esclusione - Il filtro Esclusioni consente all'utente di escludere alcuni file o alcune cartelle dall'invio (ad esempio, potrebbe essere utile escludere i file contenenti informazioni riservate, come documenti o fogli di calcolo). I file elencati non verranno mai inviati ai laboratori ESET ai fini dell'analisi, anche se contengono codice sospetto. Per impostazione predefinita, vengono esclusi i tipi di file più comuni (con estensione DOC e così via). È possibile aggiungerli all'elenco di file esclusi.

Se ESET LiveGrid® è già stato utilizzato in precedenza ed è stato disattivato, potrebbero essere ancora presenti pacchetti di dati da inviare. Tali pacchetti verranno inviati a ESET anche dopo la disattivazione. Dopo l'invio delle informazioni correnti, non verranno creati ulteriori pacchetti.

4.4.1.8.1 File sospetti

La scheda **File** nella configurazione avanzata di ESET LiveGrid® consente all'utente di configurare le modalità di invio delle minacce ai laboratori di ricerca ESET per l'analisi.

Se si rileva un file sospetto, è possibile inviarlo al laboratorio di ricerca ESET per l'analisi. Se viene individuata un'applicazione dannosa, essa verrà aggiunta al successivo aggiornamento delle firme antivirali.

Filtro di esclusione - Il Filtro di esclusione consente di escludere dall'invio determinati file/cartelle. I file elencati non verranno mai inviati ai laboratori di ricerca ESET per l'analisi, anche se contengono codice sospetto. È ad esempio utile escludere file che potrebbero contenere informazioni riservate, quali documenti o fogli di calcolo. Per impostazione predefinita, vengono esclusi i tipi di file più comuni (con estensione DOC e così via). È possibile aggiungerli alla lista degli elementi esclusi dalla scansione.

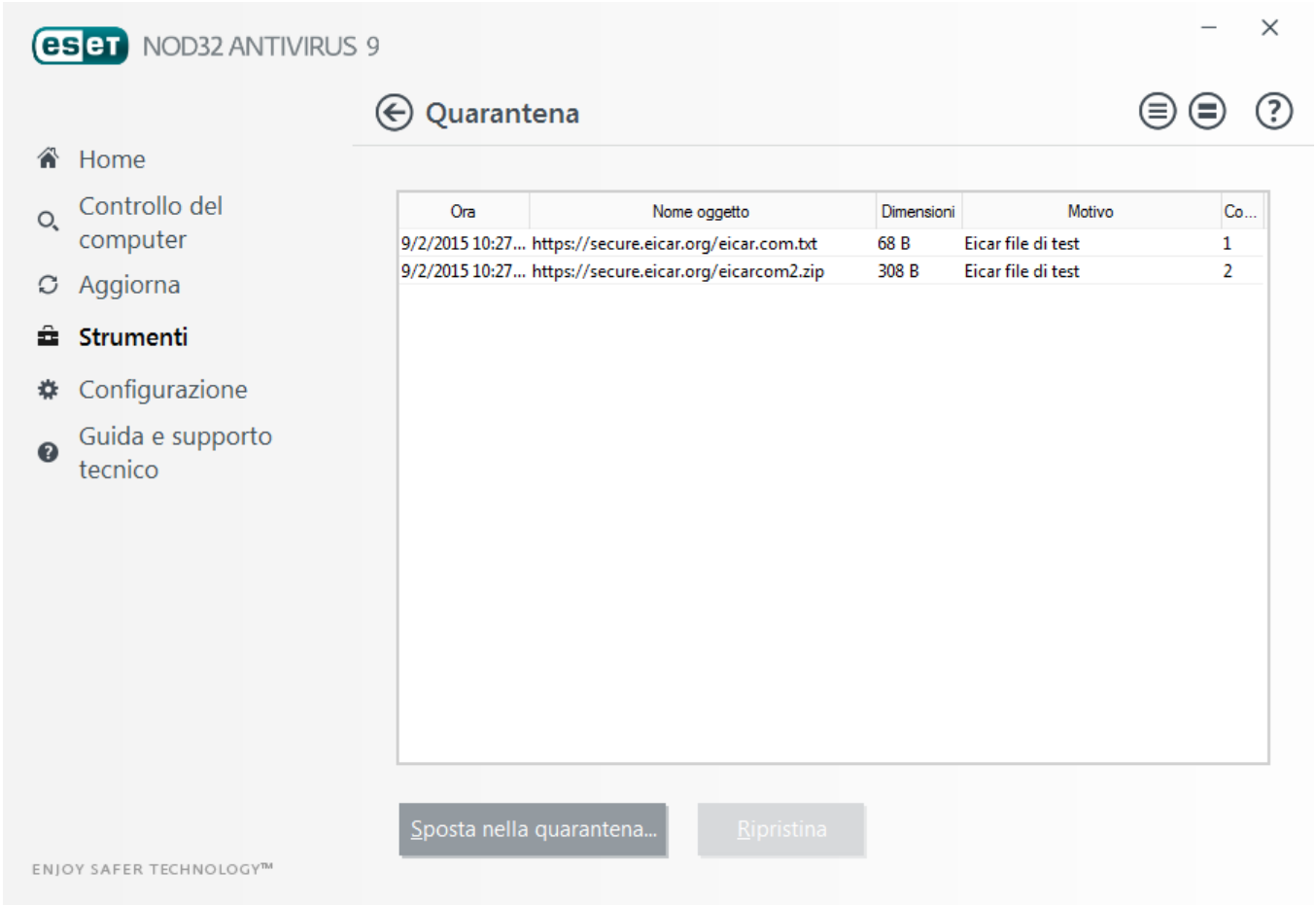
Contatto e-mail (facoltativo) - Il contatto e-mail può essere inviato insieme ai file sospetti e potrebbe essere utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Tenere presente che non si riceverà alcuna risposta da ESET, a meno che non siano richieste ulteriori informazioni.

Selezionare **Attiva registrazione** per creare un rapporto di eventi sul quale sono registrati gli invii dei file e delle informazioni statistiche. Ciò attiverà la registrazione sul Rapporto eventi durante l'invio di file o statistiche.

4.4.1.9 Quarantena

La funzione principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o, infine, se vengono erroneamente rilevati come minacce da ESET NOD32 Antivirus.

È possibile mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati al laboratorio di ricerca ESET per l'analisi.



I file salvati nella cartella della quarantena possono essere visualizzati in una tabella contenente la data e l'ora della quarantena, il percorso originale del file infetto, la dimensione in byte, il motivo (ad esempio, oggetto aggiunto dall'utente) e il numero di minacce (ad esempio, se si tratta di un archivio contenente più infiltrazioni).

Mettere file in quarantena

ESET NOD32 Antivirus mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto ad annullare questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti selezionando **Quarantena...**. In tal caso, il file originale non verrà rimosso dalla posizione di origine. Per questa operazione è possibile utilizzare anche il menu contestuale: fare clic con il pulsante destro del mouse sulla finestra **Quarantena** e selezionare l'opzione **Quarantena...**.

Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. Utilizzare a tale scopo la funzione **Ripristina**, disponibile nel menu contestuale visualizzato facendo clic con il pulsante destro del mouse su un file specifico nella finestra Quarantena. Se un file è contrassegnato come applicazione potenzialmente indesiderata, l'opzione **Ripristina ed escludi dal controllo** è attivata. Per ulteriori informazioni su questo tipo di applicazione, consultare la relativa voce del glossario. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare i file in una posizione diversa da quella di origine da cui sono stati eliminati.

NOTA: se il programma ha messo in quarantena per errore un file non dannoso, escludere il file dal controllo dopo averlo ripristinato e inviarlo al Supporto tecnico ESET.

Invio di un file dalla cartella Quarantena

Se un file sospetto che non è stato rilevato dal programma è stato messo in quarantena o se un file è stato segnalato erroneamente come infetto (ad esempio, mediante un'analisi euristica del codice) e quindi messo in quarantena, è necessario inviarlo al laboratorio antivirus ESET. Per inviare un file dalla cartella di quarantena, fare clic con il pulsante destro del mouse sul file e selezionare **Invia per analisi** dal menu contestuale.

4.4.1.10 Server proxy

Nelle reti LAN di grandi dimensioni, le comunicazioni tra il computer dell'utente e Internet possono essere mediate da un server proxy. Se si utilizza questa configurazione, è necessario definire le seguenti impostazioni. In caso contrario, il programma non sarà in grado di aggiornarsi automaticamente. In ESET NOD32 Antivirus, il server proxy può essere configurato da due sezioni differenti della struttura Configurazione avanzata.

Le impostazioni del server proxy possono innanzitutto essere configurate in **Configurazione avanzata** da **Strumenti** > **Server proxy**. Specificando il server proxy a questo livello, si definiscono le impostazioni globali del server proxy per l'intera applicazione ESET NOD32 Antivirus. Questi parametri vengono utilizzati da tutti i moduli che richiedono una connessione a Internet.

Per specificare le impostazioni del server proxy per questo livello, selezionare **Utilizza server proxy** e inserire l'indirizzo del server proxy nel campo **Server proxy**, insieme al numero di **Porta** del server proxy.

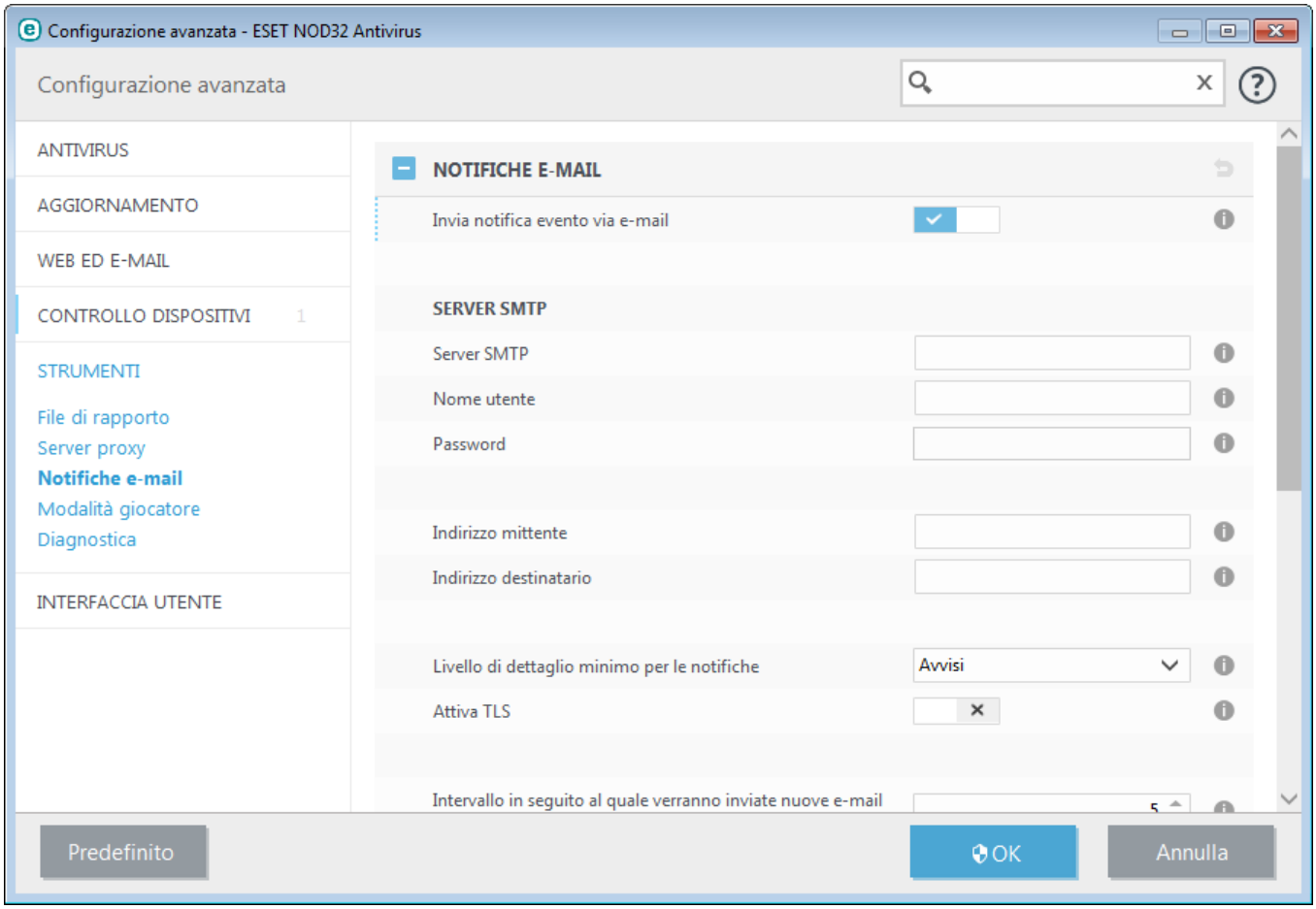
Se per la comunicazione con il server proxy è necessaria l'autenticazione, selezionare **Il server proxy richiede l'autenticazione** e inserire un **Nome utente** e una **Password** validi nei rispettivi campi. Fare clic su **Rileva** per rilevare e inserire automaticamente le impostazioni del server proxy. Verranno copiati i parametri specificati in Internet Explorer.

NOTA: nelle impostazioni del **Server proxy**, è necessario inserire manualmente il nome utente e la password.

Le impostazioni del server proxy possono anche essere definite nella Configurazione aggiornamento avanzata (**Configurazione avanzata** > **Aggiornamento** > **Proxy HTTP** selezionando **Connessione tramite un server proxy** dal menu a discesa **Modalità proxy**). Questa impostazione è applicabile al profilo di aggiornamento fornito ed è consigliata per i notebook che ricevono spesso aggiornamenti delle firme antivirali da postazioni remote. Per ulteriori informazioni su questa impostazione, consultare Configurazione aggiornamento avanzata.

4.4.1.11 Notifiche e-mail

ESET NOD32 Antivirus invia automaticamente e-mail di notifica nel caso in cui si verifichi un evento con il livello di dettaglio selezionato. Attivare **Invia notifiche di eventi via e-mail** per attivare le notifiche e-mail.



Server SMTP

Server SMTP: server SMTP utilizzato per l'invio delle notifiche (ad es. *smtp.provider.com:587*, porta predefinita 25).

NOTA: ESET NOD32 Antivirus supporta i server SMTP con crittografia TLS.

Nome utente e **password**: se il server SMTP richiede l'autenticazione, questi campi devono essere compilati con nome utente e una password validi per l'accesso al server SMTP.

Indirizzo mittente: questo campo specifica l'indirizzo del mittente che verrà visualizzato nell'intestazione delle e-mail di notifica.

Indirizzo destinatario: questo campo specifica l'indirizzo del destinatario che verrà visualizzato nell'intestazione delle e-mail di notifica.

Dal menu a discesa **Livello di dettaglio minimo per le notifiche**, è possibile selezionare il livello di dettaglio di partenza delle notifiche da inviare.

- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: registra i messaggi informativi, come gli eventi di rete non standard, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Avvisi**: registra gli errori critici e i messaggi di avviso (la funzione Anti-Stealth non funziona correttamente o l'aggiornamento non è riuscito).
- **Errori**: verranno registrati errori quali "Protezione del documento non avviata" ed errori critici.
- **Critico**: registra solo gli errori critici (errore che avvia la protezione antivirus o sistema infetto).

Attiva TLS: attiva l'invio di messaggi di avviso e notifiche supportati dalla crittografia TLS.

Intervallo in seguito al quale verranno inviate nuove e-mail di notifica (min.): intervallo in minuti in seguito al quale verranno inviate nuove notifiche all'indirizzo e-mail. Se il valore viene impostato su 0, le notifiche verranno inviate immediatamente.

Invia ciascuna notifica in un'e-mail separata: attivando questa opzione, il destinatario riceverà una nuova e-mail per ogni singola notifica. Tale operazione potrebbe determinare la ricezione di un numero elevato di messaggi e-mail in un periodo di tempo ridotto.

Formato dei messaggi

Formato dei messaggi di evento : formato dei messaggi di evento che vengono visualizzati sui computer remoti.

Formato dei messaggi di avviso per le minacce : i messaggi di avviso e notifica delle minacce presentano un formato predefinito. Si consiglia di non modificare questo formato. Tuttavia, in alcuni casi (ad esempio, se si dispone di un sistema di elaborazione delle e-mail automatizzato) potrebbe essere necessario modificare il formato dei messaggi.

Utilizza caratteri alfabetici locali: converte un messaggio e-mail nella codifica dei caratteri ANSI in base alle impostazioni della lingua di Windows (ad esempio, windows-1250). Se si lascia deselezionata questa opzione, il messaggio verrà convertito e codificato in ACSII a 7 bit (ad esempio, "á" verrà modificata in "a" e un simbolo sconosciuto verrà modificato in "?").

Utilizza codifica caratteri locali: l'origine del messaggio e-mail verrà codificata in formato QP (Quoted-printable) che utilizza i caratteri ASCII ed è in grado di trasmettere correttamente speciali caratteri nazionali tramite e-mail nel formato a 8-bit (áéíóú).

4.4.1.11.1 Formato dei messaggi

In questa sezione è possibile configurare il formato dei messaggi di evento che vengono visualizzati sui computer remoti.

Gli avvisi di minaccia e i messaggi di notifica dispongono di un formato predefinito. Si consiglia di non modificare questo formato. Tuttavia, in alcuni casi (ad esempio, se si dispone di un sistema di elaborazione della posta automatizzato) potrebbe essere necessario modificare il formato dei messaggi.

Nel messaggio, le parole chiave (stringhe separate dai segni %) vengono sostituite dalle informazioni effettive specificate. Sono disponibili le parole chiave seguenti:

- **%TimeStamp%** - Data e ora dell'evento
- **%Scanner%** - Modulo interessato
- **%ComputerName%** - Nome del computer in cui si è verificato l'avviso
- **%ProgramName%** - Programma che ha generato l'avviso
- **%InfectedObject%** - Nome del file, del messaggio, ecc. infetto
- **%VirusName%** - Identificazione dell'infezione
- **%ErrorDescription%** - Descrizione di un evento non virus

Le parole chiave **%InfectedObject%** e **%VirusName%** vengono utilizzate solo nei messaggi di allarme delle minacce, mentre **%ErrorDescription%** viene utilizzata solo nei messaggi di evento.

Utilizza caratteri alfabetici locali - Converte un messaggio e-mail nella codifica dei caratteri ANSI in base alle impostazioni della lingua di Windows (ad esempio windows-1250). Se si lascia deselezionata questa opzione, il messaggio verrà convertito e codificato in ACSII a 7 bit (ad esempio, "á" verrà modificata in "a" e un simbolo sconosciuto verrà modificato in "?").

Utilizza codifica caratteri locali - L'origine del messaggio e-mail verrà codificata in formato QP (Quoted-printable) che utilizza i caratteri ASCII ed è in grado di trasmettere correttamente speciali caratteri nazionali tramite e-mail nel formato a 8-bit (áéíóú).

4.4.1.12 Seleziona campione per analisi

La finestra di dialogo per l'invio dei file consente di inviare un file o un sito a ESET ai fini dell'analisi ed è disponibile in **Strumenti**. > **Invia campione per l'analisi**. Se è stato trovato un file con un comportamento sospetto nel computer in uso o un sito sospetto su Internet, è possibile inviarlo al laboratorio di ricerca ESET per l'analisi. Se il file si rivela essere un'applicazione o un sito Web dannoso, il suo rilevamento verrà aggiunto in un aggiornamento successivo.

In alternativa, è possibile inviare il file tramite e-mail. Se si preferisce questa opzione, comprimere il file o i file con WinRAR/ZIP, proteggere l'archivio con la password "infected" e inviarlo a campioni@eset.com. Ricordare di inserire una descrizione nel campo dell'oggetto e di fornire il maggior numero di informazioni possibile sul file (ad esempio, l'indirizzo del sito Web dal quale è stato scaricato).

NOTA: Prima di inviare un file a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:
- il file non viene rilevato
- il file viene erroneamente rilevato come una minaccia

Non verrà inviata alcuna risposta a meno che non siano richieste ulteriori informazioni ai fini dell'analisi.

Selezionare la descrizione dal menu a discesa **Motivo per l'invio del file** che si avvicina maggiormente alla propria motivazione:
- **File sospetto**
- **Sito sospetto** (un sito Web infettato da un malware),
- **File falso positivo** (file che è stato rilevato come un'infezione ma che in realtà non è infetto),
- **Sito falso positivo**
- **Altro**

File/Sito - Il percorso del file o del sito Web che si intende inviare.

E-mail contatto - Una e-mail di contatto viene inviata a ESET insieme ai file sospetti e può essere utilizzata per contattare il mittente qualora fossero necessarie ulteriori informazioni ai fini dell'analisi. L'immissione dell'indirizzo e-mail di contatto è facoltativa. ESET non invierà alcuna risposta a meno che non siano richieste ulteriori informazioni. Ogni giorno i server ESET ricevono decine di migliaia di file e non è pertanto possibile rispondere a tutti.

4.4.1.13 Aggiornamento Microsoft Windows®

La funzione di aggiornamento di Windows è un componente importante per la protezione del computer da software dannosi. Per questo motivo, è fondamentale installare gli aggiornamenti di Microsoft Windows non appena disponibili. ESET NOD32 Antivirus invia notifiche all'utente relative agli aggiornamenti mancanti in base al livello specificato. Sono disponibili i livelli seguenti:

- **Nessun aggiornamento** - Per il download non viene offerto nessun aggiornamento del sistema.
- **Aggiornamenti facoltativi** - Per il download vengono offerti aggiornamenti con priorità bassa e di livello superiore.
- **Aggiornamenti consigliati** - Per il download vengono offerti aggiornamenti contrassegnati come comuni o di livello superiore.
- **Aggiornamenti importanti** - Per il download vengono offerti aggiornamenti contrassegnati come importanti o di livello superiore.
- **Aggiornamenti critici** - Per il download vengono offerti unicamente gli aggiornamenti critici.

Fare clic su **OK** per salvare le modifiche. Dopo la verifica dello stato mediante il server di aggiornamento, viene visualizzata la finestra Aggiornamenti del sistema. Le informazioni sull'aggiornamento del sistema non saranno pertanto disponibili immediatamente dopo il salvataggio delle modifiche.

4.5 Interfaccia utente

La sezione **Interfaccia utente** consente di configurare il comportamento dell'interfaccia grafica utente (GUI) del programma.

Tramite lo strumento Grafica, è possibile regolare l'aspetto e gli effetti del programma.

Configurando gli Avvisi e notifiche, è possibile modificare il comportamento degli avvisi sulle minacce rilevate e le notifiche di sistema. in modo da adattarli alle proprie esigenze.

Se si sceglie di non visualizzare alcune notifiche, esse verranno visualizzate nell'area Finestre di notifica nascoste. In tali finestre è possibile verificarne lo stato, visualizzare ulteriori dettagli oppure rimuoverle.

Per assicurare la massima protezione del software di protezione, è possibile impedire l'esecuzione di modifiche non autorizzate proteggendo le impostazioni mediante una password tramite lo strumento Impostazione dell'accesso.

Il Menu contestuale viene visualizzato dopo aver fatto clic con il pulsante destro del mouse su un oggetto. Utilizzare questo strumento per integrare gli elementi controllo ESET NOD32 Antivirus nel menu contestuale.

4.5.1 Elementi dell'interfaccia utente

Le opzioni di configurazione dell'interfaccia utente in ESET NOD32 Antivirus consentono di modificare l'ambiente di lavoro per adattarlo alle esigenze specifiche dell'utente. Queste opzioni di configurazione sono accessibili nel ramo **Interfaccia utente** > **Elementi dell'interfaccia utente** della struttura Configurazione avanzata di ESET NOD32 Antivirus.

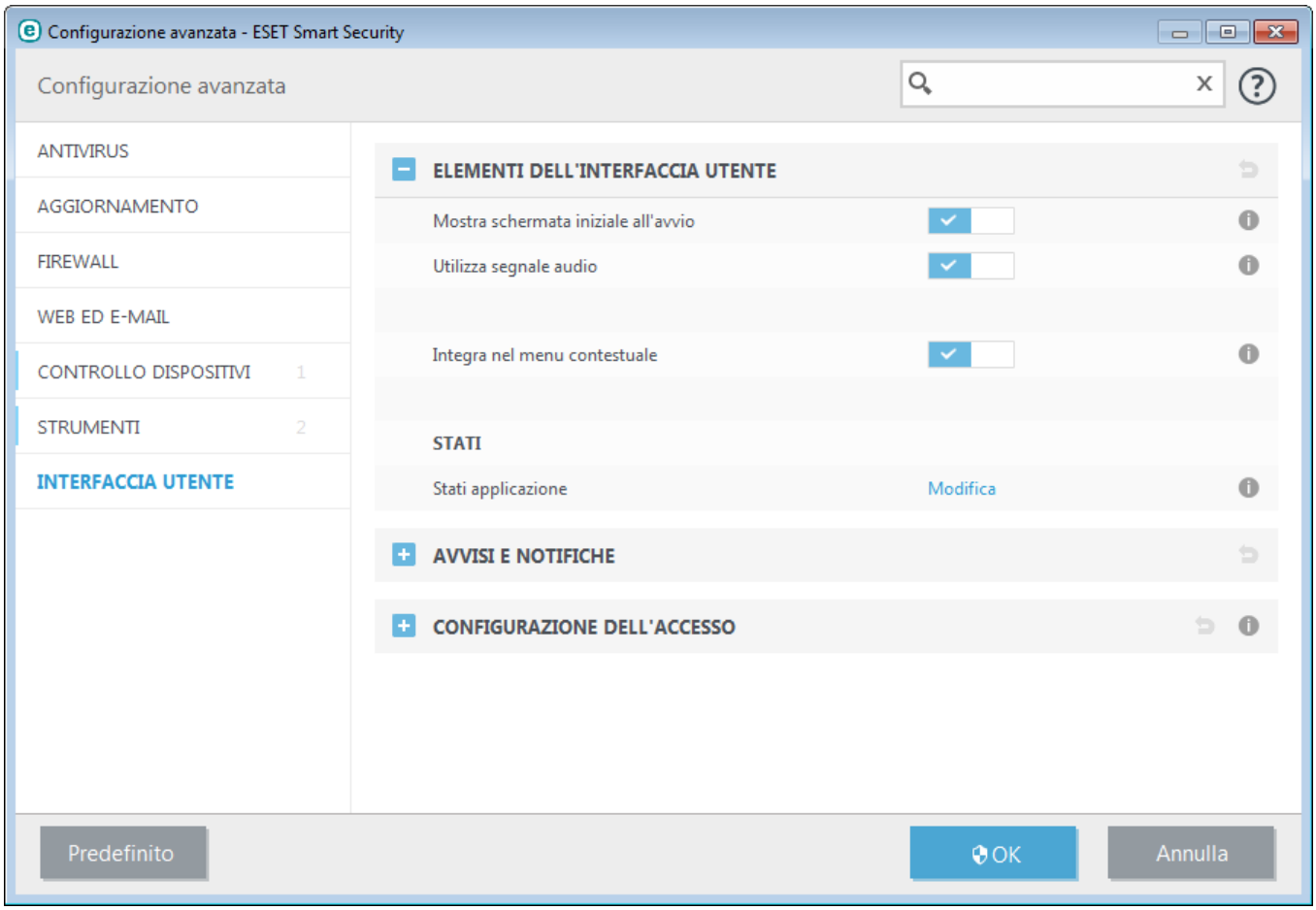
Se si desidera disattivare la schermata iniziale di ESET NOD32 Antivirus, deselezionare **Mostra schermata iniziale all'avvio**.

Per far sì che ESET NOD32 Antivirus emetta un suono al verificarsi di eventi importanti durante un controllo, ad esempio in caso di rilevamento di una minaccia o al termine del controllo, selezionare **Utilizza segnale audio**.

Integra nel menu contestuale: integra gli elementi di controllo di ESET NOD32 Antivirus nel menu contestuale.

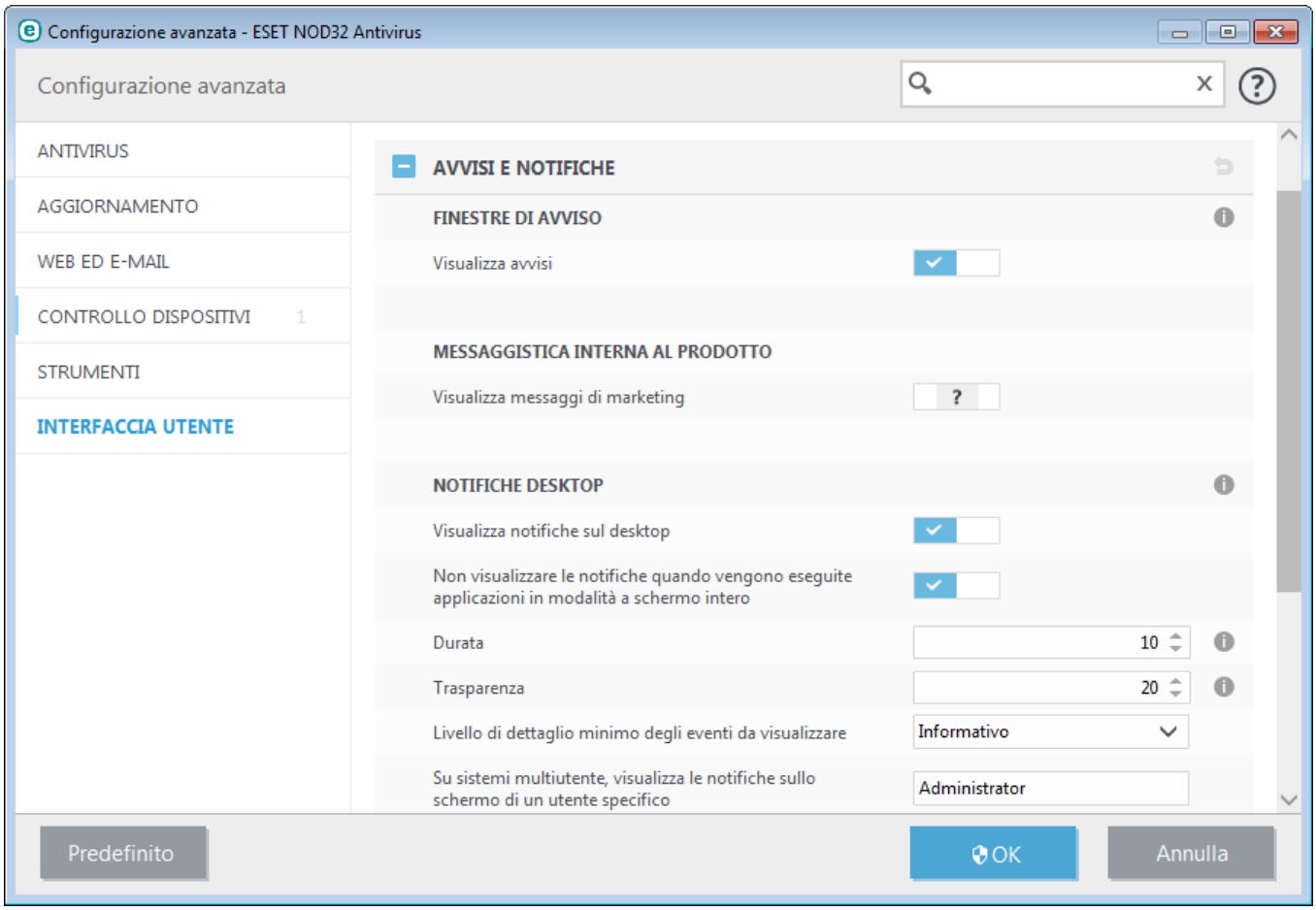
Stati

Stati applicazione: fare clic sul pulsante **Modifica** per gestire (disattivare) gli stati visualizzati nel riquadro **Stato protezione** nel menu principale.


Configurazione avanzata - ESET Smart Security
Configurazione avanzata
ANTIVIRUS
AGGIORNAMENTO
FIREWALL
WEB ED E-MAIL
CONTROLLO DISPOSITIVI 1
STRUMENTI 2
INTERFACCIA UTENTE
ELEMENTI DELL'INTERFACCIA UTENTE
Mostra schermata iniziale all'avvio
Utilizza segnale audio
Integra nel menu contestuale
STATI
Stati applicazione
Modifica
AVVISI E NOTIFICHE
CONFIGURAZIONE DELL'ACCESSO
Predefinito
OK
Annulla

4.5.2 Avvisi e notifiche

La sezione **Avvisi e notifiche** sotto a **Interfaccia utente** consente di configurare la gestione dei messaggi di avviso relativi alle minacce e delle notifiche di sistema (ad esempio, messaggi di aggiornamenti riusciti) da parte di ESET NOD32 Antivirus. È inoltre possibile impostare l'ora di visualizzazione e il livello di trasparenza delle notifiche sulla barra delle applicazioni del sistema (applicabile solo ai sistemi che supportano le notifiche sulla barra delle applicazioni).



Finestre di avviso

Disattivando **Visualizza avvisi**, tutte le finestre di avviso verranno annullate. Per tale motivo, è consigliabile eseguire tale operazione solo in un numero limitato di situazioni specifiche. Nella maggior parte dei casi, si consiglia di non modificare l'impostazione predefinita (opzione attivata).

Messaggistica interna al prodotto

Visualizza messaggi di marketing - Il servizio di messaggistica interna al prodotto è stato ideato allo scopo di informare gli utenti in merito alle novità di ESET e di inviare altri tipi di comunicazioni. Disattivare questa opzione qualora non si desideri ricevere messaggi di marketing.

Notifiche desktop

Le notifiche visualizzate sul desktop e i suggerimenti sono forniti esclusivamente a titolo informativo e non richiedono l'interazione dell'utente. Vengono visualizzati nell'area di notifica posta nell'angolo in basso a destra della schermata. Per attivare la visualizzazione delle notifiche sul desktop, selezionare **Visualizza notifiche sul desktop**.

Attivare **Non visualizzare le notifiche quando vengono eseguite applicazioni in modalità a schermo intero** per eliminare tutte le notifiche non interattive. È possibile modificare opzioni più dettagliate, ad esempio l'orario di visualizzazione della notifica e la trasparenza della finestra seguendo le istruzioni fornite di seguito.

Il menu a discesa **Livello di dettaglio minimo degli eventi da visualizzare** consente all'utente di selezionare il livello di gravità degli avvisi e delle notifiche da visualizzare. Sono disponibili le seguenti opzioni:

- **Diagnostica**: registra le informazioni necessarie ai fini dell'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativo**: registra i messaggi informativi, compresi quelli relativi agli aggiornamenti riusciti, e tutti i record indicati in precedenza.
- **Allarmi**: consente di registrare errori critici e messaggi di allarme.
- **Errori**: verranno registrati errori quali "Errore durante il download del file" ed errori critici.
- **Critica**: registra solo gli errori critici (errore che avvia la protezione antiviruse così via).

L'ultima funzione in questa sezione consente di configurare la destinazione delle notifiche in un ambiente multiutente. Nel campo **In sistemi multiutente, visualizza le notifiche sullo schermo di questo utente** viene specificato l'utente che riceverà le notifiche di sistema e di altro tipo sui sistemi che consentono la connessione simultanea di più utenti. In genere si tratta di un amministratore di sistema o di rete. Questa opzione è utile soprattutto per i server di terminali, a condizione che tutte le notifiche di sistema vengano inviate all'amministratore.

Finestre di messaggio

Per chiudere automaticamente le finestre popup dopo un determinato periodo di tempo, selezionare **Chiudi automaticamente le finestre di messaggio**. Se non vengono chiuse manualmente, le finestre di avviso vengono chiuse automaticamente una volta trascorso il periodo di tempo specificato.

Messaggi di conferma: consente all'utente di visualizzare un elenco di messaggi di conferma che è possibile decidere di visualizzare o non visualizzare.

4.5.2.1 Configurazione avanzata

Nel menu a discesa **Livello di dettaglio minimo degli eventi da visualizzare** è possibile selezionare il livello iniziale di gravità degli avvisi e delle notifiche da visualizzare.

- **Diagnostica** - Registra tutte le informazioni necessarie per l'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativi** - Messaggi di record informativi che includono gli aggiornamenti riusciti e tutti i record indicati in precedenza.
- **Allarmi** - Consente di registrare errori critici e messaggi di allarme.
- **Errori** - Verranno registrati errori quali *"Errore durante il download del file"* ed errori critici.
- **Critici** - Registra solo gli errori critici (errore che avvia la protezione antiviruse così via).

L'ultima funzione in questa sezione consente di configurare la destinazione delle notifiche in un ambiente multi-utente. Nel campo **In sistemi multiutente, visualizza le notifiche sullo schermo di questo utente** viene specificato l'utente che riceverà le notifiche di sistema e di altro tipo sui sistemi che consentono la connessione simultanea di più utenti. In genere si tratta di un amministratore di sistema o di rete. Questa opzione è utile soprattutto per i server di terminali, a condizione che tutte le notifiche di sistema vengano inviate all'amministratore.

4.5.3 Finestre di notifica nascoste

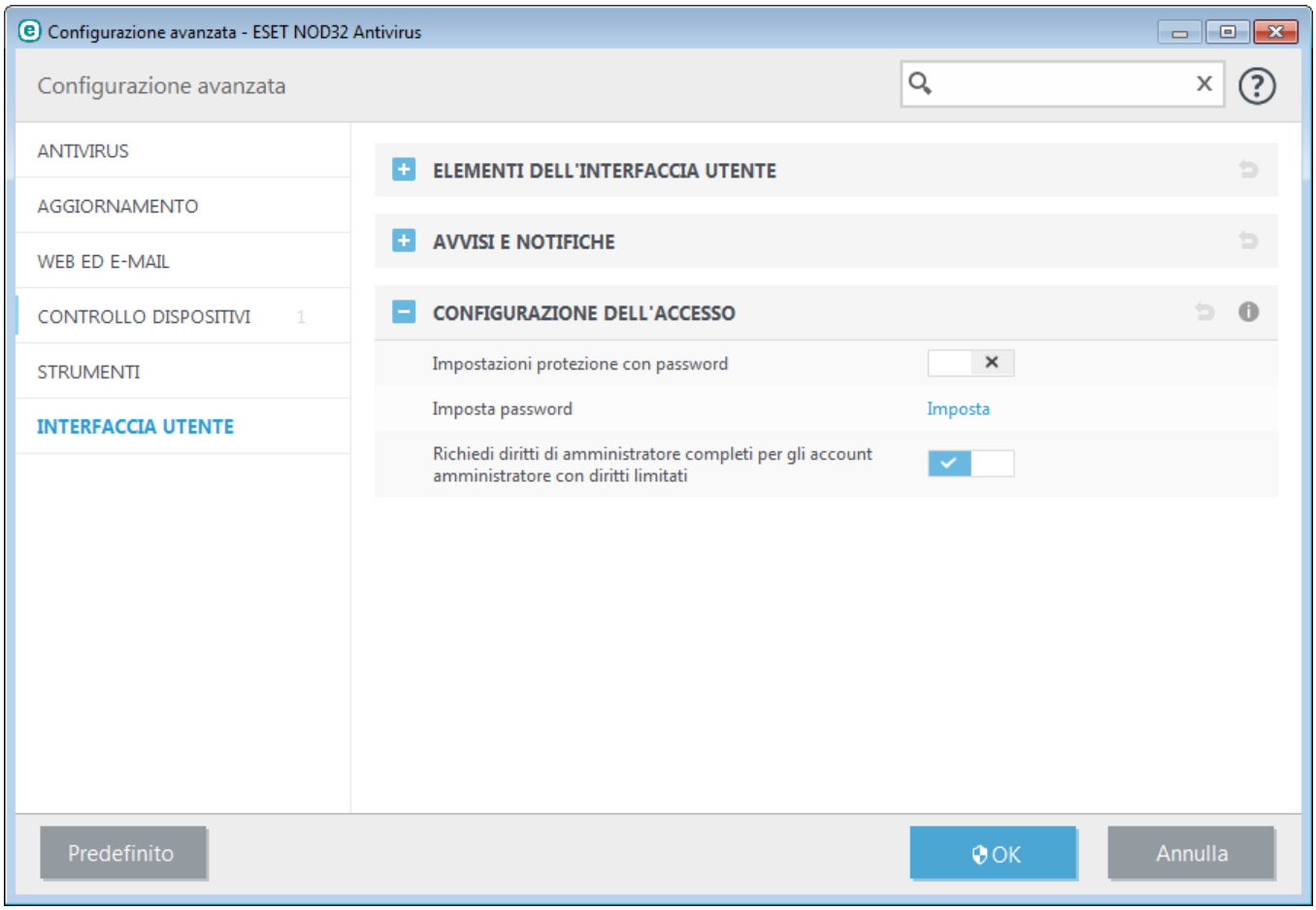
Se per le finestre di notifica (avvisi) visualizzate in precedenza è stata selezionata l'opzione **Non visualizzare più questo messaggio**, questa notifica verrà visualizzata nell'elenco delle finestre di notifica nascoste. Le azioni eseguite automaticamente vengono visualizzate nella colonna **Conferma**.

Mostra - Mostra un'anteprima delle finestre di notifica al momento non visualizzate e per le quali è configurata un'azione automatica.

Rimuovi - Rimuove voci dall'elenco **Finestre di messaggio nascoste**. Tutte le finestre di notifica rimosse dall'elenco verranno visualizzate nuovamente.

4.5.4 Configurazione dell'accesso

Le impostazioni ESET NOD32 Antivirus rappresentano una parte cruciale dei criteri di protezione. Modifiche non autorizzate potrebbero mettere a rischio la stabilità e la protezione del sistema. Per evitare modifiche non autorizzate, i parametri di configurazione di ESET NOD32 Antivirus possono essere protetti con password.



Impostazioni protette con password: indica le impostazioni relative alla password. Fare clic per aprire la finestra di configurazione della password.

Per impostare o modificare una password al fine di proteggere i parametri di configurazione, fare clic su **Imposta**.

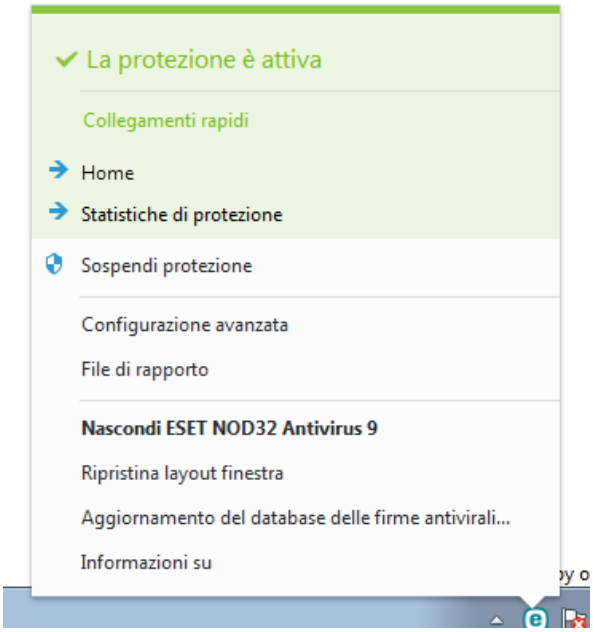
Richiedi diritti di amministratore completi per gli account con diritti limitati - Selezionare questa opzione per richiedere all'utente corrente (nel caso non disponga dei diritti di amministratore) di inserire un nome utente e una password di amministratore per la modifica di alcuni parametri del sistema (analogo a Controllo dell'account utente (UAC) in Windows Vista e Windows 7). Tali modifiche includono la disattivazione dei moduli di protezione. Sui sistemi Windows XP, in cui l'UAC non è in esecuzione, gli utenti avranno a disposizione l'opzione **Richiedi diritti di amministratore (sistema senza supporto Controllo dell'account utente)**.

Solo per Windows XP:

Richiedi diritti di amministratore (sistema senza supporto Controllo dell'account utente): attivare questa opzione per ottenere il prompt di ESET NOD32 Antivirus relativo alle credenziali dell'amministratore.

4.5.5 Menu del programma

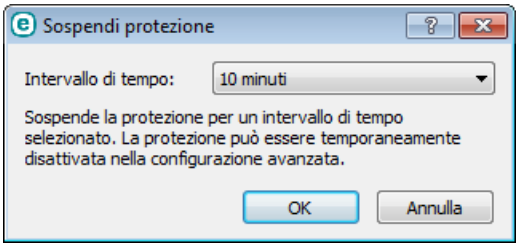
Alcune delle principali opzioni di configurazione e funzionalità sono disponibili facendo clic con il pulsante destro del mouse sull'icona della barra delle applicazioni .



Collegamenti rapidi: consente di visualizzare le parti di ESET NOD32 Antivirus che vengono utilizzate più frequentemente. È possibile accedervi rapidamente dal menu del programma.

Sospendi protezione: consente di visualizzare la finestra di dialogo di conferma per disattivare la Protezione antivirus e antispyware che protegge da attacchi dannosi al sistema controllando file e comunicazioni Web ed e-mail.

Il menu a discesa **Intervallo di tempo** rappresenta l'intervallo di tempo durante il quale la Protezione antivirus e antispyware verrà disattivata.


Sospendi protezione
Intervallo di tempo:
10 minuti
Sospende la protezione per un intervallo di tempo selezionato. La protezione può essere temporaneamente disattivata nella configurazione avanzata.
OK
Annulla

Configurazione avanzata: selezionare questa opzione per accedere alla struttura **Configurazione avanzata**. Vi sono anche altri modi per aprire la Configurazione avanzata, ad esempio, premendo il tasto F5 oppure accedendo a **Configurazione** > **Configurazione avanzata**.

File di rapporto - I File di rapporto contengono informazioni relative agli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate.

Nascondi ESET NOD32 Antivirus: nasconde la finestra di ESET NOD32 Antivirus dalla schermata.

Ripristina layout finestra - Ripristina le dimensioni predefinite e la posizione sullo schermo della finestra di ESET NOD32 Antivirus.

Attivazione del prodotto... - Selezionare questa opzione se non è ancora stato attivato il prodotto di protezione ESET oppure inserire nuovamente le credenziali di attivazione del prodotto dopo aver rinnovato la licenza.

Aggiornamento database firme antivirali: avvia l'aggiornamento del database delle firme antivirali per garantire il livello di protezione stabilito dall'utente contro codici dannosi.

Informazioni su - Vengono fornite informazioni sul sistema, dettagli sulla versione installata di ESET NOD32 Antivirus e sui relativi moduli di programma installati. In questa sezione è anche possibile trovare la data di

scadenza della licenza e le informazioni relative al sistema operativo e alle risorse di sistema.

4.5.6 Menu contestuale

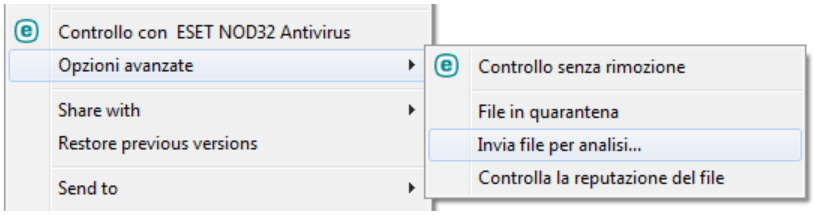
Il menu contestuale viene visualizzato dopo aver fatto clic con il pulsante destro del mouse su un oggetto. Nel menu sono elencate tutte le azioni che è possibile eseguire su un oggetto.

È possibile integrare gli elementi controllo ESET NOD32 Antivirus nel menu contestuale. Sono disponibili opzioni di configurazione più dettagliate per questa funzionalità nella struttura Configurazione avanzata in **Interfaccia utente** > **Menu contestuale**.

Integra nel menu contestuale - Integrare gli elementi controllo ESET NOD32 Antivirus nel menu contestuale.

Nel menu a discesa **Tipo di menu** sono disponibili le seguenti opzioni:

- **Completo (esegui prima controllo)** - Attiva tutte le opzioni del menu contestuale. Nel menu principale verrà visualizzato **Controllo senza pulizia con ESET NOD32 Antivirus** come prima opzione e **Controllo e pulizia** come seconda opzione.
- **Completo (esegui prima pulitura)** - Attiva tutte le opzioni del menu contestuale. Nel menu principale verrà visualizzato **Controllo con ESET NOD32 Antivirus** come prima opzione e **Controllo senza pulizia** come seconda opzione.



- **Solo controllo** - Nel menu contestuale verrà visualizzato solo **Controlla senza pulizia con ESET NOD32 Antivirus**.
- **Solo pulizia** - Nel menu contestuale verrà visualizzato solo **Controllo con ESET NOD32 Antivirus**.

5. Utente avanzato

5.1 Gestione profili

La Gestione profili viene utilizzata in due modi all'interno di ESET NOD32 Antivirus: nella sezione **Controllo computer su richiesta** e nella sezione **Aggiorna**.

Controllo del computer

È possibile salvare i parametri di scansione preferiti per i controlli futuri. È consigliabile creare un profilo di scansione differente (con diversi oggetti da controllare, metodi di scansione e altri parametri) per ciascuna scansione utilizzata abitualmente.

Per creare un nuovo profilo, aprire la finestra Configurazione avanzata (F5) e fare clic su **Antivirus** > **Controllo computer su richiesta** > **Di base** > **Elenco di profili**. Nella finestra **Gestione profili** è disponibile un menu a discesa **Profili selezionati** contenente i profili di scansione esistenti e l'opzione per crearne di nuovi. Per ricevere assistenza durante la creazione di un profilo di controllo adatto alle proprie esigenze, consultare la sezione Configurazione parametri motore ThreatSense contenente una descrizione di ciascun parametro di configurazione del controllo.

Esempio: si supponga di voler creare il proprio profilo di controllo e che la configurazione **Controlla il computer in uso** sia appropriata solo in parte, in quanto non si desidera eseguire il controllo di eseguibili compressi o di applicazioni potenzialmente pericolose e si intende applicare l'opzione **Massima pulizia**. Inserire il nome del nuovo profilo nella finestra **Gestione profili** e fare clic su **Aggiungi**. Selezionare il nuovo profilo dal menu a discesa **Profilo selezionato**, modificare i parametri rimanenti in base alle proprie esigenze e fare clic su **OK** per salvare il nuovo profilo.

Aggiorna

L'editor dei profili nella sezione Impostazione aggiornamento consente agli utenti di creare nuovi profili di aggiornamento. Creare e utilizzare i profili personalizzati (diversi dal **Profilo personale** predefinito) solo se il computer utilizza vari metodi di connessione ai server di aggiornamento.

Ad esempio, un computer portatile che si connette normalmente a un server locale (Mirror) nella rete locale ma scarica gli aggiornamenti direttamente dai server di aggiornamento ESET durante la disconnessione (trasferta di lavoro) potrebbe utilizzare due profili: il primo per connettersi al server locale e il secondo per connettersi ai server ESET. Dopo aver configurato questi profili, accedere a **Strumenti** > **Pianificazione attività** e modificare i parametri delle attività di aggiornamento. Indicare un profilo come principale e l'altro come secondario.

Profilo selezionato - Il profilo di aggiornamento attualmente utilizzato. Per modificarlo, scegliere un profilo dal menu a discesa.

Aggiungi... - Consente di creare nuovi profili di aggiornamento.

Nella parte inferiore della finestra è visualizzato l'elenco dei profili esistenti.

5.2 Tasti di scelta rapida

Per una migliore navigazione del prodotto ESET, è possibile utilizzare i seguenti tasti di scelta rapida:

F1	apre le pagine della Guida
F5	apre la Configurazione avanzata
Tasti Su/Giù	navigazione all'interno delle voci del prodotto
-	comprime i nodi della struttura Configurazione avanzata
TAB	sposta il cursore in una finestra
Esc	chiude la finestra di dialogo attiva

5.3 Diagnostica

La diagnostica fornisce dump sulle interruzioni delle applicazioni correlate ai processi ESET (ad esempio, *ekrn*). In caso di interruzione di un'applicazione, verrà generato un dump, che aiuta gli sviluppatori a eseguire il debug e correggere vari problemi di ESET NOD32 Antivirus. Fare clic sul menu a discesa accanto a **Tipo di dump** e selezionare una delle tre opzioni disponibili:

- Selezionare **Disattiva** (impostazione predefinita) per disattivare questa funzionalità.
- **Mini**: registra il minor numero di informazioni utili che potrebbero contribuire all'identificazione del motivo alla base dell'arresto inaspettato dell'applicazione. Questo tipo di file dump risulta utile in caso di limitazioni di spazio. Tuttavia, a causa delle informazioni limitate incluse, gli errori che non sono stati causati direttamente dalla minaccia in esecuzione quando si è verificato il problema potrebbero non essere rilevati a seguito di un'analisi del file in questione.
- **Completo**: registra tutti i contenuti della memoria di sistema quando l'applicazione viene interrotta inaspettatamente. Un dump memoria completo può contenete dati estrapolati dai processi in esecuzione quando è stato raccolto il dump di memoria.

Attiva registrazione avanzata filtraggio protocolli: registra tutti i dati che attraversano il motore di filtraggio protocolli in formato PCAP. Tale operazione consente agli sviluppatori di diagnosticare e correggere problemi correlati al filtraggio protocolli.

I file di rapporto sono disponibili in:
C:\Programmi\ESET\ESET Smart Security\Diagnostica su Windows Vista e versioni successive o *C:\Documents and Settings\All Users\...* sulle versioni precedenti di Windows.

Directory di destinazione - Directory nella quale verrà generato il dump durante l'arresto imprevisto.

Apri cartella diagnostica: fare clic su **Apri** per aprire questa directory in una nuova finestra di *Windows Explorer*.

5.4 Importa ed esporta impostazioni

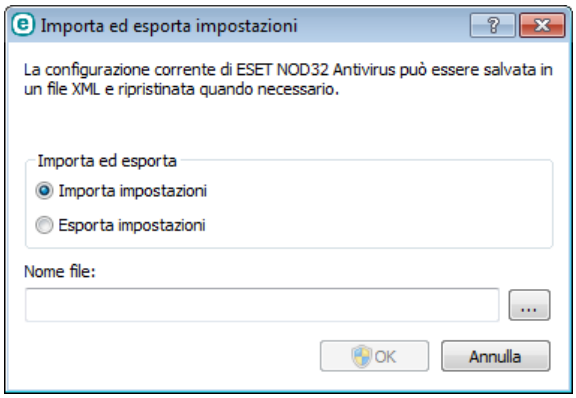
È possibile importare o esportare il file di configurazione personalizzato in formato .xml di ESET NOD32 Antivirus dal menu **Configurazione**.

I file di importazione e di esportazione sono utili se si necessita effettuare un backup della configurazione corrente di ESET NOD32 Antivirus da utilizzare in un secondo momento. L'opzione di esportazione delle impostazioni è utile anche per gli utenti che desiderano utilizzare la configurazione preferita su più sistemi. In tal modo, sarà possibile importare facilmente un file *.xml* per il trasferimento di queste impostazioni.

L'importazione della configurazione è molto semplice. Nella finestra principale del programma, fare clic su **Configurazione** > **Importa ed esporta impostazioni**, quindi selezionare **Importa impostazioni**. Inserire il percorso del file di configurazione o fare clic sul pulsante **...** per ricercare il file di configurazione che si vuole importare.

Le operazioni per esportare una configurazione sono molto simili. Nella finestra principale del programma, fare clic su **Configurazione** > **Importa ed esporta impostazioni**. Selezionare **Esporta impostazioni** e inserire il percorso del file di configurazione (ad esempio, *export.xml*). Utilizzare il browser per selezionare un percorso sul computer in cui salvare il file di configurazione.

NOTA: durante l'esportazione delle impostazioni potrebbe comparire un errore se non si dispone degli idonei diritti di scrittura del file esportato nella directory specificata.



5.5 Rilevamento stato inattivo

Le impostazioni del rilevamento stato inattivo possono essere configurate nella sezione **Configurazione avanzata** in **Strumenti** > **Rilevamento stato inattivo**. Queste impostazioni specificano l'attivazione del Controllo stato inattivo se:

- è attivo lo screen saver,
- il computer è bloccato,
- un utente si disconnette.

Utilizzare le caselle di controllo per attivare o disattivare i vari metodi di attivazione del rilevamento dello stato inattivo.

5.6 ESET SysInspector

5.6.1 Introduzione a ESET SysInspector

L'applicazione ESET SysInspector ispeziona il computer in modo approfondito e visualizza i dati raccolti in modo globale. La raccolta di informazioni su driver e applicazioni, su connessioni di rete o importanti voci di registro semplifica il controllo di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

È possibile accedere a ESET SysInspector in due modi: dalla versione integrata nelle soluzioni ESET Security o scaricando gratuitamente la versione indipendente (SysInspector.exe) dal sito Web ESET. Le funzionalità e i comandi di entrambe le versioni sono identici. L'unica differenza consiste nella gestione dei risultati. La versione indipendente e quella integrata consentono entrambe di esportare snapshot del sistema su un file *XML* e salvarli su disco. La versione integrata consente tuttavia anche di memorizzare gli snapshot di sistema direttamente in **Strumenti** > **ESET SysInspector** (tranne ESET Remote Administrator). Per ulteriori informazioni, vedere la sezione ESET SysInspector come componente di ESET NOD32 Antivirus.

È necessario attendere qualche minuto per consentire a ESET SysInspector di controllare il computer. A seconda della configurazione hardware, del sistema operativo e del numero di applicazioni installate nel computer in uso, questa operazione potrebbe richiedere da 10 secondi ad alcuni minuti.

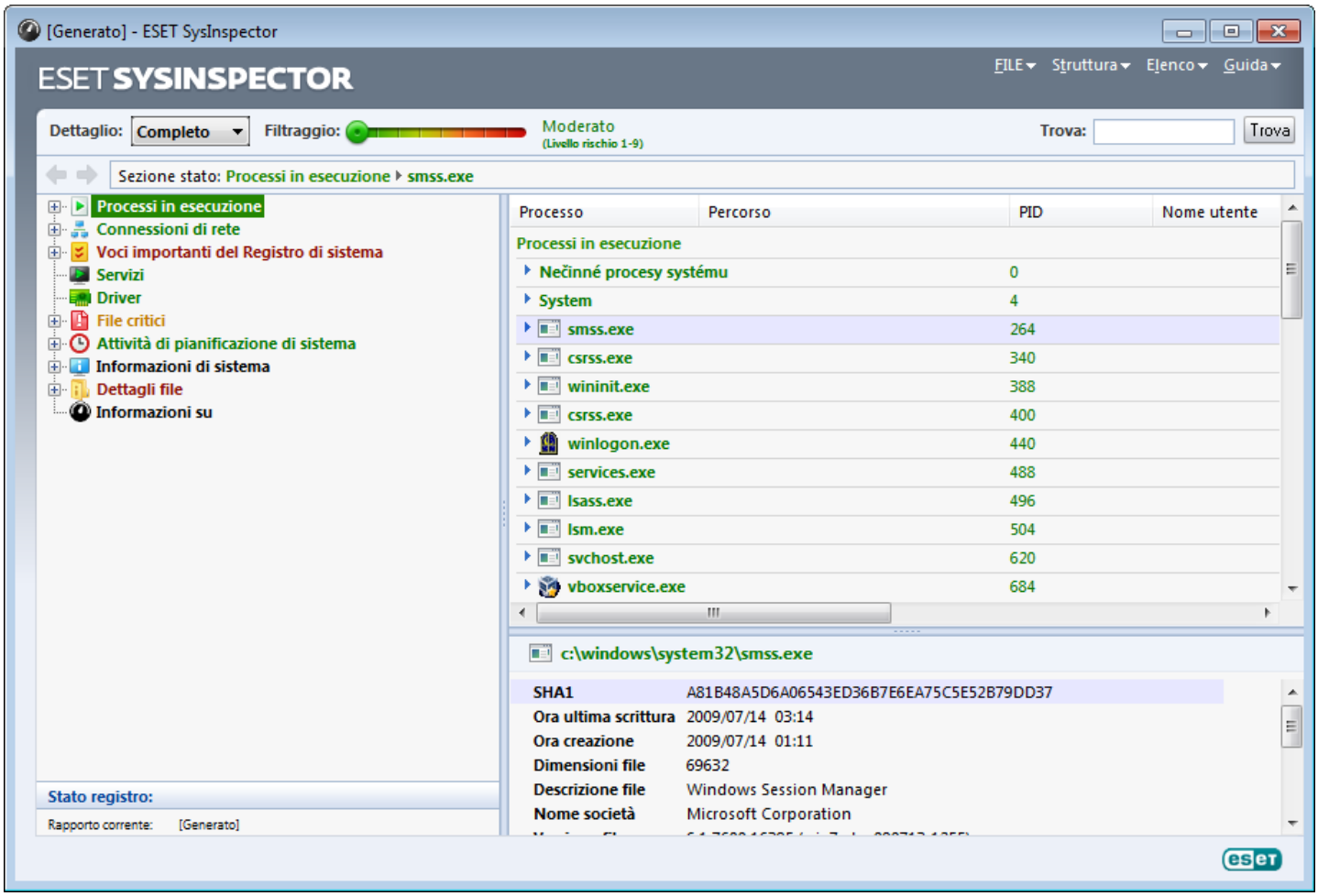
5.6.1.1 Avvio di ESET SysInspector

Per avviare ESET SysInspector è sufficiente eseguire il file eseguibile *SysInspector.exe* scaricato dal sito Web ESET. Se è già installata una delle soluzioni ESET Security, è possibile eseguire ESET SysInspector direttamente dal menu Start (fare clic su **Programmi** > **ESET** > **ESET NOD32 Antivirus**).

Si prega di attendere che l'applicazione abbia esaminato il sistema in uso. Questa operazione potrebbe richiedere diversi minuti.

5.6.2 Interfaccia utente e utilizzo dell'applicazione

Per chiarezza, la finestra principale del programma è stata divisa in quattro sezioni principali: i comandi del programma sono posizionati nella parte superiore della finestra; a sinistra viene visualizzata la finestra di spostamento, a destra è disponibile la finestra Descrizione e, infine, nella parte inferiore della schermata, viene visualizzata la finestra Dettagli. Nella sezione Stato registro sono elencati i parametri principali di un rapporto (filtro usato, tipo di filtro, se il rapporto è il risultato di un confronto e così via).



5.6.2.1 Comandi del programma

La presente sezione contiene la descrizione di tutti i comandi del programma disponibili in ESET SysInspector.

File

Selezionare **File** per memorizzare lo stato attuale del sistema per un'analisi futura oppure aprire un rapporto precedentemente archiviato. Ai fini della pubblicazione, è consigliabile generare un rapporto **Idoneo all'invio**. In questo formato, nel rapporto vengono omesse informazioni riservate (nome utente attuale, nome computer, nome dominio, privilegi utente attuale, variabili d'ambiente e così via).

NOTA: è possibile aprire i rapporti di ESET SysInspector precedentemente archiviati trascinandoli nella finestra principale del programma.

Struttura

Consente di espandere o chiudere tutti i nodi e di esportare le sezioni selezionate sullo script di servizio.

Elenco

Contiene funzioni per uno spostamento più pratico all'interno del programma e varie altre funzioni, ad esempio la ricerca di informazioni su Internet.

Guida

Contiene informazioni sull'applicazione e sulle relative funzioni.

Dettaglio

Questa impostazione influenza le informazioni visualizzate nella finestra principale del programma al fine di semplificarne l'utilizzo. Nella modalità "Base" si ha accesso alle informazioni utilizzate per trovare soluzioni a problemi comuni del sistema. Nella modalità "Media" il programma visualizza i dettagli meno utilizzati, mentre nella modalità "Completa", ESET SysInspector mostra tutte le informazioni necessarie alla soluzione di problemi specifici.

Filtraggio

Il filtraggio elementi viene utilizzato soprattutto per individuare file o voci di registro sospetti all'interno del sistema. Regolando il cursore, è possibile filtrare gli elementi in base al livello di rischio. Se il cursore si trova all'estrema sinistra (Livello di rischio 1) vengono visualizzati tutti gli elementi. Spostando il cursore a destra, il programma esclude tutti gli elementi meno rischiosi rispetto al livello di rischio corrente, consentendo di visualizzare solo gli elementi che risultano più sospetti rispetto al livello visualizzato. Quando il cursore si trova all'estrema destra, il programma visualizza solo gli elementi dannosi conosciuti.

Tutti gli elementi contrassegnati con un livello di rischio compreso tra 6 e 9 rappresentano un rischio per la sicurezza. Se ESET SysInspector ha rilevato un elemento di questo tipo, si consiglia di eseguire il controllo del sistema con ESET Online Scanner, se non si utilizza una soluzione di protezione di ESET. ESET Online Scanner è un servizio gratuito.

NOTA: il Livello di rischio di un elemento può essere determinato rapidamente confrontandone il colore con quello del cursore Livello di rischio.

Confronta

Durante il confronto di due rapporti, è possibile scegliere di visualizzare tutti gli elementi, solo gli elementi aggiunti, solo gli elementi rimossi o solo gli elementi sostituiti.

Trova

L'opzione Cerca può essere utilizzata per individuare rapidamente un elemento specifico in base al nome o parte di esso. I risultati della richiesta di ricerca vengono visualizzati nella finestra Descrizione.

Ritorna

Facendo clic sulle frecce indietro o avanti, è possibile tornare alle informazioni precedentemente visualizzate nella finestra Descrizione. È possibile utilizzare i tasti Cancella e Barra spaziatrice anziché fare clic su Avanti e Indietro.

Sezione stato

Visualizza il nodo corrente nella finestra di spostamento.

Importante: gli elementi evidenziati in rosso sono sconosciuti. Per tale motivo, il programma li segna come potenzialmente pericolosi. Se un elemento è segnalata in rosso, non significa automaticamente che sia possibile eliminare il file. Prima di procedere all'eliminazione, assicurarsi che i file siano effettivamente pericolosi o non necessari.

5.6.2.2 Navigare in ESET SysInspector

ESET SysInspector divide vari tipi di informazioni in numerose sezioni di base, dette nodi. Se disponibili, ulteriori dettagli saranno visualizzabili espandendo ciascun nodo nei relativi sottonodi. Per espandere o comprimere un nodo, fare doppio clic sul nome del nodo oppure fare clic su ⊞ o ⊟ accanto al nome del nodo. Spostandosi nella struttura ad albero di nodi e sottonodi della finestra di spostamento, sono disponibili vari dettagli su ciascun nodo presente nella finestra Descrizione. Navigando tra gli elementi della finestra Descrizione, è possibile visualizzare ulteriori dettagli per ciascun elemento nella finestra Dettagli.

Di seguito vengono riportate le descrizioni dei nodi principali presenti nella finestra di spostamento e le relative informazioni delle finestre Descrizione e Dettagli.

Processi in esecuzione

Questo nodo contiene informazioni sulle applicazioni e sui processi in esecuzione durante la generazione del rapporto. Nella finestra Descrizione sono disponibili dettagli aggiuntivi su ciascun processo, ad esempio le librerie dinamiche utilizzate dal processo e la loro posizione nel sistema, il nome del produttore dell'applicazione e il livello di rischio del file.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

NOTA: un sistema operativo è basato su diversi componenti kernel, costantemente in esecuzione, che forniscono funzioni fondamentali e di base per le altre applicazioni utente. In alcuni casi, tali processi sono visualizzati nello strumento ESET SysInspector con il percorso file preceduto da \??\. Quei simboli forniscono un'ottimizzazione per i processi in questione prima di avviarli e risultano sicuri per il sistema.

Connessioni di rete

La finestra Descrizione contiene un elenco di processi e applicazioni che comunicano sulla rete utilizzando il protocollo selezionato nella finestra di spostamento (TCP o UDP), unitamente all'indirizzo remoto a cui è collegata l'applicazione. È inoltre possibile verificare gli indirizzi IP dei server DNS.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

Voci importanti del Registro di sistema

Contiene un elenco delle voci di registro selezionate che sono spesso correlate a vari problemi del sistema, ad esempio quelle indicano i programmi di avvio, oggetti browser helper (BHO) e così via.

Nella finestra Descrizione è possibile visualizzare i file correlati a voci di registro specifiche. Nella finestra Dettagli è possibile visualizzare maggiori informazioni.

Servizi

La finestra Descrizione contiene un elenco di file registrati come Servizi Windows. Nella finestra Dettagli è possibile controllare il modo in cui è impostato l'avvio del servizio insieme ai dettagli specifici del file.

Driver

Un elenco di driver installati nel sistema.

File critici

Nella finestra Descrizione è visualizzato il contenuto dei file critici relativi al sistema operativo Microsoft Windows.

Attività di pianificazione di sistema

Contiene un elenco delle attività avviate dall'Utilità di pianificazione di Windows a un orario/intervallo specificato.

Informazioni di sistema

Contiene informazioni dettagliate sull'hardware e sul software, oltre a informazioni sulle variabili d'ambiente

impostate, sui diritti utente e sui rapporti eventi di sistema.

Dettagli file

Un elenco di file di sistema importanti e di file presenti nella cartella Programmi. Per maggiori informazioni sui file in questione, fare riferimento alle finestre Descrizione e Dettagli.

Informazioni su

Informazioni sulla versione di ESET SysInspector ed elenco dei moduli del programma.

5.6.2.2.1 Tasti di scelta rapida

I tasti di scelta rapida che possono essere utilizzati con ESET SysInspector includono:

File

Ctrl+O	apre il rapporto esistente
Ctrl+S	salva i rapporti creati

Genera

Ctrl+G	genera uno snapshot di stato computer standard
Ctrl+H	genera uno snapshot di stato computer che potrebbe registrare anche informazioni sensibili

Filtraggio elementi

1, O	non a rischio, visualizzati gli elementi con livello di rischio 1-9
2	non a rischio, visualizzati gli elementi con livello di rischio 2-9
3	non a rischio, visualizzati gli elementi con livello di rischio 3-9
4, U	sconosciuto, visualizzati gli elementi con livello di rischio 4-9
5	sconosciuto, visualizzati gli elementi con livello di rischio 5-9
6	sconosciuto, visualizzati gli elementi con livello di rischio 6-9
7, B	a rischio, visualizzati gli elementi con livello di rischio 7-9
8	a rischio, visualizzati gli elementi con livello di rischio 8-9
9	a rischio, visualizzati gli elementi con livello di rischio 9
-	diminuisce il livello di rischio
+	aumenta il livello di rischio
Ctrl+9	modalità di filtraggio, livello uguale o più alto
Ctrl+0	modalità di filtraggio, solo livello uguale

Visualizza

Ctrl+5	visualizza per fornitore, tutti i fornitori
Ctrl+6	visualizza per fornitore, solo Microsoft
Ctrl+7	visualizza per fornitore, tutti gli altri fornitori
Ctrl+3	mostra tutti i dettagli
Ctrl+2	livello di dettaglio medio
Ctrl+1	visualizzazione di base
Cancella	indietro di un passaggio
Barra spaziatrice	avanti di un passaggio
Ctrl+W	espande la struttura
Ctrl+Q	comprime la struttura

Altri comandi

Ctrl+T	va alla posizione originale dell'elemento dopo averlo selezionato nei risultati di ricerca
Ctrl+P	visualizza informazioni di base su un elemento
Ctrl+A	visualizza informazioni complete di un elemento
Ctrl+C	copia la struttura dell'elemento attuale
Ctrl+X	copia gli elementi

Ctrl+B	trova su Internet le informazioni sui file selezionati
Ctrl+L	apre la cartella dove si trova il file selezionato
Ctrl+R	apre la voce corrispondente nell'editor del Registro di sistema
Ctrl+Z	copia un percorso di un file (se l'elemento è relativo a un file)
Ctrl+F	passa al campo di ricerca
Ctrl+D	chiude i risultati di ricerca
Ctrl+E	esegue lo script di servizio

Confronto

Ctrl+Alt+O	apre il rapporto originale/comparativo
Ctrl+Alt+R	annulla il confronto
Ctrl+Alt+1	visualizza tutti gli elementi
Ctrl+Alt+2	visualizza solo gli elementi aggiunti, il rapporto mostrerà gli elementi presenti nel rapporto attuale
Ctrl+Alt+3	visualizza solo gli elementi rimossi, il rapporto mostrerà gli elementi presenti nel rapporto precedente
Ctrl+Alt+4	visualizza solo gli elementi sostituiti (compresi i file)
Ctrl+Alt+5	visualizza solo le differenze tra i rapporti
Ctrl+Alt+C	visualizza il confronto
Ctrl+Alt+N	visualizza il rapporto attuale
Ctrl+Alt+P	apre il rapporto precedente

Varie

F1	visualizza la guida
Alt+F4	chiude il programma
Alt+Maiusc+F4	chiude il programma senza chiedere
Ctrl+I	statistiche registro

5.6.2.3 Confronta

La funzione Confronta consente di mettere a confronto due rapporti esistenti. Il risultato di questa funzione è una serie di elementi non comuni ai due rapporti. È la soluzione ideale se si desidera individuare le modifiche nel sistema ed è un utile strumento per il rilevamento di codice dannoso.

Dopo l'avvio, l'applicazione crea un nuovo rapporto, visualizzato in una nuova finestra. Fare clic su **File** > **Salva rapporto** per salvare un rapporto in un file. I file di rapporto possono essere aperti e visualizzati in un secondo momento. Per aprire un rapporto esistente, fare clic su **File** > **Apri rapporto**. Nella finestra principale del programma, ESET SysInspector visualizza sempre un rapporto alla volta.

Il confronto tra due rapporti offre il vantaggio di visualizzare un rapporto attualmente attivo e uno salvato in un file. Per confrontare i rapporti, fare clic su **File** > **Confronta rapporto** e scegliere **Seleziona file**. Il rapporto selezionato verrà confrontato con quello attivo nelle finestre principali del programma. Nel rapporto comparativo saranno visualizzate solo le differenze tra i due.

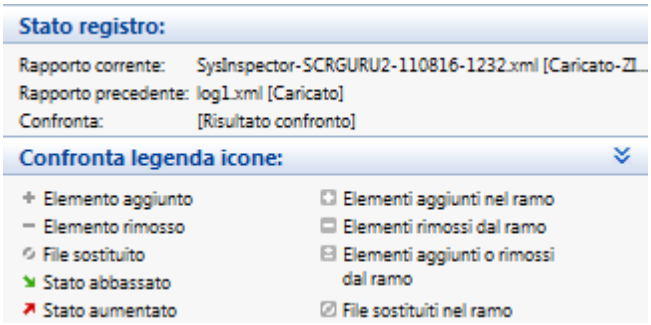
NOTA: se si mettono a confronto due file di rapporto, facendo clic su **File** > **Salva rapporto** e salvandoli in un file ZIP, verranno salvati entrambi i file. Se si apre il file in un secondo momento, i rapporti contenuti verranno automaticamente messi a confronto.

Accanto agli elementi visualizzati, ESET SysInspector mostra i simboli che identificano le differenze tra i rapporti confrontati.

Descrizione di tutti i simboli che possono essere visualizzati accanto agli elementi:

- + nuovo valore, non presente nel rapporto precedente
- la sezione della struttura contiene nuovi valori
- – valore rimosso, presente solo nel rapporto precedente
- la sezione della struttura contiene i valori rimossi
- il valore/file è stato modificato
- la sezione della struttura contiene valori/file modificati
- il livello di rischio è diminuito/era più alto nel precedente rapporto
- il livello di rischio è aumentato/era più basso nel precedente rapporto

Nella sezione di descrizione visualizzata nell'angolo in basso a sinistra vengono descritti tutti i simboli e mostrati i nomi dei rapporti confrontati.



Qualsiasi rapporto comparativo può essere salvato in un file e aperto successivamente.

Esempio

Generare e salvare un rapporto, registrando le informazioni originali sul sistema, in un file denominato previous.xml. Dopo aver effettuato le modifiche al sistema, aprire ESET SysInspector e attendere che venga eseguito un nuovo rapporto. Salvarlo in un file denominato *current.xml*.

Al fine di rilevare le modifiche tra i due rapporti, fare clic su **File** > **Confronta rapporti**. Il programma crea un rapporto comparativo che visualizza solo le differenze tra i due.

È possibile ottenere lo stesso risultato utilizzando la seguente opzione della riga di comando:

SysIsnpector.exe current.xml previous.xml

5.6.3 Parametri della riga di comando

ESET SysInspector supporta la generazione di rapporti dalla riga di comando con i seguenti parametri:

/gen	genera rapporto direttamente dalla riga di comando senza avviare l'interfaccia grafica utente (GUI)
/privacy	genera rapporto omettendo le informazioni sensibili
/zip	salva rapporto in un archivio zip compresso
/silent	non visualizzare finestra di avanzamento durante la creazione del rapporto dalla riga di comando
/blank	avvia ESET SysInspector senza generare/caricare il rapporto

Esempi

Utilizzo:
`Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]`

Per caricare un rapporto specifico direttamente nel browser, utilizzare: *SysInspector.exe .\clientlog.xml*
Per generare il rapporto dalla riga di comando, utilizzare: *SysInspector.exe /gen=.\mynewlog.xml*
Per generare un rapporto escludendo le informazioni sensibili direttamente in un file compresso, utilizzare: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Per confrontare due file di rapporto ed esaminare le differenze, utilizzare: *SysInspector.exe new.xml old.xml*

NOTA: Se il nome di un file/cartella contiene uno spazio vuoto, è necessario inserirlo tra virgolette.

5.6.4 Script di servizio

Lo script di servizio è uno strumento utile per i clienti che utilizzano ESET SysInspector in quanto consente di rimuovere facilmente gli oggetti indesiderati dal sistema.

Lo script di servizio consente all'utente di esportare l'intero rapporto di ESET SysInspector o le parti selezionate. Al termine dell'esportazione, è possibile selezionare gli oggetti indesiderati da eliminare. È quindi possibile eseguire il rapporto modificato per eliminare gli oggetti contrassegnati.

Lo script di servizio è adatto agli utenti avanzati che hanno già esperienza nella diagnostica dei problemi del sistema. Le modifiche effettuate da persone non qualificate potrebbero causare danni al sistema operativo.

Esempio

Se si sospetta che il computer sia infettato da un virus non rilevato dal programma antivirus, attenersi alle seguenti istruzioni dettagliate:

1. Eseguire ESET SysInspector per generare un nuovo snapshot del sistema.
2. Selezionare il primo elemento della sezione a sinistra (nella struttura ad albero), premere Shift ed evidenziare l'ultimo elemento per selezionarli tutti.
3. Fare clic con il pulsante destro del mouse sugli oggetti selezionati e scegliere **Esporta sezioni selezionate a script di servizio**.
4. Gli oggetti selezionati verranno esportati in un nuovo rapporto.
5. Questo è il passaggio più importante dell'intera procedura: aprire il nuovo rapporto e cambiare l'attributo - in + per tutti gli oggetti che si desidera rimuovere. Fare attenzione a non contrassegnare file/oggetti importanti del sistema operativo.
6. Aprire ESET SysInspector, fare clic su **File** > **Esegui script di servizio** e immettere il percorso dello script.
7. Fare clic su **OK** per eseguire lo script.

5.6.4.1 Generazione dello script di servizio

Per generare uno script, fare clic con il pulsante destro del mouse su qualsiasi voce della struttura del menu (nel riquadro a sinistra) nella finestra principale di ESET SysInspector. Selezionare l'opzione **Esporta tutte le sezioni a script di servizio** o **Esporta sezioni selezionate a script di servizio** nel menu contestuale.

NOTA: non è possibile esportare lo script di servizio quando vengono confrontati due rapporti.

5.6.4.2 Struttura dello script di servizio

Nella prima riga dell'intestazione dello script sono disponibili informazioni sulla versione del motore (ev), sulla versione dell'interfaccia utente (gv) e sulla versione del rapporto (lv). Questi dati possono essere utilizzati per tenere traccia delle possibili variazioni nel file XML che genera lo script e prevenire eventuali incoerenze durante l'esecuzione. Non modificare questa parte dello script.

La restante parte del file è suddivisa in sezioni in cui è possibile modificare gli elementi (indicare quelli che saranno elaborati dallo script). È possibile contrassegnare gli elementi da elaborare sostituendo il carattere "-" davanti a un elemento con il carattere "+". Le sezioni dello script sono separate tra loro mediante una riga vuota. A ogni sezione viene assegnato un numero e un titolo.

01) Processi in esecuzione

Questa sezione contiene un elenco di tutti i processi in esecuzione nel sistema. Ogni processo è identificato mediante il proprio percorso UNC e, successivamente, dal rispettivo codice hash CRC16 tra asterischi (*).

Esempio:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Nell'esempio, è stato selezionato un processo, module32.exe (contrassegnato dal carattere "+"). Il processo

terminerà all'esecuzione dello script.

02) Moduli caricati

In questa sezione sono contenuti i moduli di sistema attualmente in uso.

Esempio:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Nell'esempio, il modulo khbekhb.dll è stato contrassegnato con "+". All'esecuzione dello script, i processi che eseguono tale modulo specifico verranno riconosciuti e interrotti.

03) Connessioni TCP

Questa sezione contiene informazioni sulle connessioni TCP esistenti.

Esempio:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

All'esecuzione dello script, verrà individuato il proprietario del socket nelle connessioni TCP contrassegnate e il socket verrà interrotto, liberando le risorse del sistema.

04) Endpoint UDP

Questa sezione contiene informazioni sugli endpoint UDP esistenti.

Esempio:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

All'esecuzione dello script, verrà isolato il proprietario del socket sugli endpoint UDP contrassegnati e il socket verrà interrotto.

05) Voci server DNS

Questa sezione contiene informazioni sulla configurazione del server DNS corrente.

Esempio:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

All'esecuzione dello script, le voci del server DNS contrassegnate verranno rimosse.

06) Voci importanti del Registro di sistema

Questa sezione contiene informazioni su importanti voci del Registro di sistema.

Esempio:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

All'esecuzione dello script, le voci contrassegnate verranno eliminate, ridotte a valori a 0 byte o ripristinate sui valori predefiniti. L'azione da eseguire su una particolare voce dipende dalla categoria della voce stessa e dal valore principale nel Registro di sistema specifico.

07) Servizi

In questa sezione sono riportati i servizi registrati all'interno del sistema.

Esempio:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

All'esecuzione dello script, i servizi contrassegnati e i relativi servizi dipendenti verranno interrotti e disinstallati.

08) Driver

In questa sezione sono riportati i driver installati.

Esempio:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando si esegue lo script, i driver selezionati verranno arrestati. Tenere presente che alcuni driver non possono essere arrestati.

09) File critici

Questa sezione contiene informazioni sui file critici per il corretto funzionamento del sistema operativo.

Esempio:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Gli elementi selezionati saranno eliminati o ripristinati sui valori originali.

10) Attività pianificate

Questa sezione contiene informazioni sulle attività pianificate.

Esempio:

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.6.4.3 Esecuzione degli script di servizio

Contrassegnare tutti gli elementi desiderati, quindi salvare e chiudere lo script. Eseguire lo script modificato direttamente dalla finestra principale di ESET SysInspector selezionando l'opzione **Esegui script di servizio** dal menu File. All'apertura di uno script, verrà visualizzato il seguente messaggio: **Eseguire lo script di servizio "%Scriptname %"?** Dopo aver confermato, verrà visualizzato un altro messaggio per segnalare che lo script di servizio che si sta cercando di eseguire non è stato firmato. Fare clic su **Esegui** per avviare lo script.

Verrà visualizzata una finestra di dialogo per confermare la corretta esecuzione dello script.

Se lo script è stato eseguito solo parzialmente, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio è stato eseguito parzialmente. Visualizzare il rapporto degli errori?** Selezionare **Sì** per visualizzare un rapporto completo degli errori in cui sono indicate le operazioni non eseguite.

Se lo script non viene riconosciuto, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio selezionato non è firmato. L'esecuzione di script sconosciuti o non firmati potrebbe causare seri danni ai dati nel computer. Eseguire lo script e le azioni?** Ciò potrebbe essere causato da incoerenze all'interno dello script (intestazione danneggiata, titolo della sezione danneggiato, linea vuota tra le sezioni e così via). È possibile riaprire il file script e correggere gli errori all'interno dello script o creare un nuovo script di servizio.

5.6.5 Domande frequenti

ESET SysInspector richiede privilegi di amministratore per l'esecuzione?

Anche se per eseguire ESET SysInspector non sono necessari privilegi di amministratore, alcune informazioni raccolte possono essere visualizzate solo da un account amministratore. Eseguendo il programma come utente standard o utente con restrizioni, si raccoglieranno meno informazioni sull'ambiente operativo in uso.

ESET SysInspector crea un file di rapporto?

ESET SysInspector può creare un file di rapporto della configurazione del proprio computer. Per salvarne uno, fare clic su **File** > **Salva rapporto** nella finestra principale del programma. I rapporti vengono salvati nel formato XML. Per impostazione predefinita, i file vengono salvati nella directory *%USERPROFILE%\Documenti*, con una convenzione di denominazione file "SysInpsector-%COMPUTERNAME%-AAMMGG-HHMM.XML". Se preferibile, è possibile modificare la posizione e il nome del file di rapporto prima di salvarlo.

Come si visualizza il file di rapporto di ESET SysInspector?

Per visualizzare un file di rapporto creato da ESET SysInspector, eseguire il programma e fare clic su **File** > **Apri rapporto** nella finestra principale del programma. È anche possibile trascinare i file di rapporto all'interno dell'applicazione ESET SysInspector. Se è necessario consultare frequentemente i file di rapporto di ESET SysInspector, è consigliabile creare un collegamento sul Desktop al file SYSINSPECTOR.EXE, quindi sarà sufficiente trascinare i file di rapporto sopra di esso per poterli visualizzare. Per motivi di protezione, in Windows Vista/7 la funzione di trascinamento della selezione tra finestre con differenti autorizzazioni di protezione potrebbe non essere disponibile.

È disponibile una specifica per il formato del file di rapporto? E per quanto riguarda un SDK?

Attualmente non è disponibile né una specifica per il file di rapporto né un SDK, in quanto il programma è ancora in fase di sviluppo. Dopo il rilascio del programma, potrebbero essere forniti sulla base dei commenti e delle richieste dei clienti.

In che modo ESET SysInspector valuta il rischio di un determinato oggetto?

Nella maggior parte dei casi, ESET SysInspector assegna livelli di rischio agli oggetti (file, processi, chiavi di registro, ecc.), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ogni oggetto e quindi ne valutano le potenzialità come attività dannosa. Sulla base di tali euristiche, agli oggetti viene assegnato un livello di rischio da 1 - Non a rischio (verde) a 9 - A rischio (rosso). Nel riquadro di spostamento a sinistra, le sezioni sono colorate sulla base del livello di rischio più elevato di un oggetto al loro interno.

Un livello di rischio "6 - Sconosciuto (rosso)" significa che un oggetto è pericoloso?

Le valutazioni di ESET SysInspector non garantiscono che un oggetto sia dannoso. Questa affermazione dovrebbe essere eseguita da un esperto di sicurezza. ESET SysInspector è progettato per fornire una rapida valutazione agli esperti di sicurezza, in modo da informarli su quali oggetti del sistema potrebbero richiedere una loro ulteriore analisi in presenza di comportamento anomalo.

Perché ESET SysInspector si collega a Internet quando viene avviato?

Al pari di molte applicazioni, ESET SysInspector è provvisto di firma digitale, un certificato che garantisce la pubblicazione del software da parte di ESET e l'assenza di alterazione dello stesso. Al fine di verificare il certificato, il sistema operativo contatta un'autorità di certificazione per verificare l'identità dell'autore del software. Si tratta di una procedura comune eseguita su tutti i programmi con firma digitale eseguiti in Microsoft Windows.

Cos'è la tecnologia Anti-Stealth?

La tecnologia Anti-Stealth assicura un efficace rilevamento di rootkit.

Se il sistema viene attaccato da codice dannoso che si comporta come un rootkit, l'utente può essere esposto al rischio di perdita o furto dei dati. In assenza di uno strumento speciale anti-rootkit, è quasi impossibile rilevarli.

Perché a volte i file contrassegnati come "Firmati da MS", hanno contemporaneamente un "Nome aziendale" differente?

Quando si cerca di identificare la firma digitale di un file eseguibile, ESET SysInspector verifica innanzitutto se nel file è incorporata una firma digitale. Se viene trovata una firma digitale, il file verrà convalidato usando tali informazioni. Se la firma digitale non viene trovata, ESI inizia a ricercare il file CAT corrispondente (Catalogo di protezione - *%systemroot%\system32\catroot*) contenente informazioni sul file eseguibile elaborato. Nel caso in cui dovesse trovare il file CAT appropriato, nel processo di convalida del file eseguibile verrà applicata la firma digitale di tale file CAT.

Per tale motivo, a volte i file contrassegnati come "Firmati da MS", hanno contemporaneamente un "Nome aziendale" differente.

Esempio:

Windows 2000 include l'applicazione HyperTerminal nel percorso *C:\Programmi\Windows NT*. Il file eseguibile dell'applicazione principale non è firmato a livello digitale, ma ESET SysInspector lo contrassegna come file firmato da Microsoft. Ciò dipende da un riferimento in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* che punta a *C:\Programmi\Windows NT\hypertrm.exe* (il principale file eseguibile dell'applicazione HyperTerminal) e *sp4.cat* è firmato a livello digitale da Microsoft.

5.6.6 ESET SysInspector come componente di ESET NOD32 Antivirus

Per aprire la sezione ESET SysInspector in ESET NOD32 Antivirus, fare clic su **Strumenti** > **ESET SysInspector**. Il sistema di gestione della finestra di ESET SysInspector è simile a quello dei rapporti di scansione del computer o delle attività pianificate. Tutte le operazioni con gli snapshot del sistema (crea, visualizza, confronta, rimuovi ed esporta) sono accessibili con pochi clic.

La finestra di ESET SysInspector contiene informazioni di base sugli snapshot creati, quali data e ora di creazione, breve commento, nome dell'utente che ha creato lo snapshot e stato dello snapshot.

Per eseguire il confronto, la creazione o l'eliminazione degli snapshot, utilizzare i pulsanti corrispondenti nella parte inferiore della finestra di ESET SysInspector. Quelle opzioni sono disponibili anche dal menu contestuale. Per visualizzare lo snapshot di sistema selezionato, scegliere **Mostra** dal menu contestuale. Per esportare lo snapshot selezionato in un file, fare clic con il pulsante destro del mouse, quindi selezionare **Esporta...**.

Di seguito viene fornita una descrizione dettagliata delle opzioni disponibili:

- **Confronta** - Consente di confrontare due rapporti esistenti. È idonea se si desidera rilevare le modifiche tra il rapporto attuale e uno precedente. Per utilizzare questa opzione, selezionare due snapshot da mettere a confronto.
- **Crea...** - Consente di creare un nuovo record. È prima necessario inserire un breve commento sul record. Per visualizzare lo stato di avanzamento della procedura di creazione dello snapshot (relativamente allo snapshot in corso di generazione), fare riferimento alla colonna **Stato**. Tutti gli snapshot completati sono contrassegnati dallo stato **Creato**.
- **Elimina/Elimina tutto** - Consente di rimuovere le voci dall'elenco.
- **Esporta...** - Salva la voce selezionata in un file XML (anche in una versione compressa).

5.7 Riga di comando

Il modulo antivirus di ESET NOD32 Antivirus può essere avviato dalla riga di comando, manualmente con il comando "ecls" oppure con un file batch ("bat"). Utilizzo dello scanner della riga di comando ESET:

```
ecls [OPTIONS..] FILES..
```

È possibile utilizzare i parametri e le opzioni riportati di seguito quando viene eseguita una scansione su richiesta dalla riga di comando:

Opzioni

/base-dir=FOLDER carica moduli da CARTELLA

/quar-dir=FOLDER	CARTELLA di quarantena
/exclude=MASK	escludi dalla scansione i file corrispondenti a MASCHERA
/subdir	esegui controllo delle sottocartelle (impostazione predefinita)
/no-subdir	non eseguire controllo delle sottocartelle
/max-subdir-level=LEVEL	sottolivello massimo delle cartelle all'interno di cartelle su cui eseguire la scansione
/symlink	segui i collegamenti simbolici (impostazione predefinita)
/no-symlink	ignora collegamenti simbolici
/ads	esegui la scansione di ADS (impostazione predefinita)
/no-ads	non eseguire la scansione di ADS
/log-file=FILE	registra output nel FILE
/log-rewrite	sovrascrivi il file di output (impostazione predefinita: aggiungi)
/log-console	registra l'output nella console (impostazione predefinita)
/no-log-console	non registrare l'output nella console
/log-all	registra anche file puliti
/no-log-all	non registrare file puliti (impostazione predefinita)
/aind	mostra indicatore di attività
/auto	controlla e disinfetta automaticamente tutti i dischi locali

Opzioni scanner

/files	esegui controllo dei file (impostazione predefinita)
/no-files	non eseguire controllo dei file
/memory	esegui scansione della memoria
/boots	esegui la scansione dei settori di avvio
/no-boots	non eseguire la scansione dei settori di avvio (impostazione predefinita)
/arch	esegui controllo degli archivi (impostazione predefinita)
/no-arch	non eseguire controllo degli archivi
/max-obj-size=SIZE	esegui solo la scansione dei file inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/max-arch-level=LEVEL	sottolivello massimo degli archivi all'interno di archivi (archivi nidificati) su cui eseguire la scansione
/scan-timeout=LIMIT	esegui scansione degli archivi per LIMITE secondi al massimo
/max-arch-size=SIZE	esegui la scansione dei file di un archivio solo se inferiori a DIMENSIONE (impostazione predefinita 0 = illimitato)
/max-sfx-size=SIZE	esegui la scansione dei file di un archivio autoestraente solo se inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/mail	esegui la scansione dei file di e-mail (impostazione predefinita)
/no-mail	non eseguire controllo dei file di e-mail
/mailbox	esegui la scansione delle caselle di posta (impostazione predefinita)
/no-mailbox	non eseguire la scansione delle caselle di posta
/sfx	esegui la scansione degli archivi autoestraenti (impostazione predefinita)
/no-sfx	non eseguire controllo degli archivi autoestraenti
/rtp	esegui la scansione degli eseguibili compressi (impostazione predefinita)
/no-rtp	non eseguire la scansione degli eseguibili compressi
/unsafe	esegui la scansione delle applicazioni potenzialmente pericolose
/no-unsafe	non eseguire la scansione delle applicazioni potenzialmente pericolose (impostazione predefinita)
/unwanted	esegui la scansione delle applicazioni potenzialmente indesiderate
/no-unwanted	non eseguire la scansione delle applicazioni potenzialmente indesiderate (impostazione predefinita)
/suspicious	ricerca applicazioni sospette (impostazione predefinita)
/no-suspicious	non ricercare applicazioni sospette
/pattern	utilizza le firme digitali (impostazione predefinita)
/no-pattern	non utilizzare le firme digitali
/heur	attiva l'euristica (impostazione predefinita)
/no-heur	disattiva l'euristica
/adv-heur	attiva l'euristica avanzata (impostazione predefinita)
/no-adv-heur	disattiva l'euristica avanzata
/ext=EXTENSIONS	esegui scansione solo di ESTENSIONI delimitate da due punti
/ext-exclude=EXTENSIONS	escludi dal controllo le ESTENSIONI delimitate da due punti

/clean-mode=MODE utilizza la MODALITÀ pulizia per gli oggetti infetti

Sono disponibili le seguenti opzioni:

- **nessuna** - Non verrà eseguita alcuna pulizia automatica.
- **standard** (impostazione predefinita) - ecls.exe tenterà di eseguire la pulizia o l'eliminazione automatica di file infetti.
- **massima** - ecls.exe tenterà di eseguire la pulizia o l'eliminazione automatica di file infetti senza l'intervento dell'utente (all'utente non verrà richiesto di confermare l'eliminazione dei file).
- **rigorosa** - ecls.exe eliminerà i file senza tentare di effettuarne la pulizia e indipendentemente dalla loro tipologia.
- **eliminazione** - ecls.exe eliminerà i file senza tentare di effettuarne la pulizia, ma eviterà di eliminare file sensibili come quelli del sistema Windows.

/quarantena copiare i file infettati (se puliti) in Quarantena (integra l'azione eseguita durante la pulizia)

/no-quarantena non copiare file infettati in Quarantena

Opzioni generali

/help mostra guida ed esci

/version mostra informazioni sulla versione ed esci

/preserve-time mantieni indicatore data e ora dell'ultimo accesso

Codici di uscita

0	nessuna minaccia rilevata
1	minaccia rilevata e pulita
10	impossibile controllare alcuni file (potrebbero essere minacce)
50	trovata minaccia
100	errore

NOTA: i codici di uscita superiori a 100 indicano che non è stata eseguita la scansione del file, il quale potrebbe quindi essere infetto.

6. Glossario

6.1 Tipi di infiltrazioni

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

6.1.1 Virus

Un virus è un pezzo di codice dannoso che è pre-incorporato o viene aggiunto ai file esistenti nel computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro. Il termine "virus" viene spesso utilizzato in maniera errata per indicare qualsiasi tipo di minaccia. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di "malware" (software dannoso).

I virus attaccano principalmente i file eseguibili e i documenti. In breve, un virus funziona nel seguente modo: dopo aver eseguito un file infetto, il codice dannoso viene chiamato ed eseguito prima dell'esecuzione dell'applicazione originale. Un virus può infettare qualsiasi file sul quale l'utente corrente dispone dei diritti di scrittura.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché sono in grado di eliminare deliberatamente i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo consiste esclusivamente nell'infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

Se il computer è stato infettato da un virus e non è possibile rimuoverlo, inviarlo ai laboratori di ricerca ESET ai fini di un esame accurato. In alcuni casi, i file infetti possono essere modificati a un livello tale da impedirne la pulizia. In questo caso, è necessario sostituire i file con una copia non infetta.

6.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite la rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di propagarsi autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi e-mail all'interno della lista dei contatti degli utenti oppure sfruttano le vulnerabilità delle applicazioni di rete.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, possono espandersi in tutto il mondo entro poche ore o persino pochi minuti dal rilascio. Questa capacità di replicarsi in modo indipendente e rapido li rende molto più pericolosi rispetto ad altri tipi di malware.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

6.1.3 Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di minacce che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli così a eseguirli.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- **Downloader** - Programmi dannosi in grado di scaricare altre minacce da Internet.
- **Dropper** - Programmi dannosi in grado di installare sui computer compromessi altri tipi di malware.
- **Backdoor** - Programmi dannosi che comunicano con gli autori degli attacchi remoti, consentendo loro di ottenere l'accesso al computer e assumerne il controllo.
- **Keylogger** (registratore delle battute dei tasti) - Un programma che registra ogni battuta di tasto effettuata da un utente e che invia le informazioni agli autori degli attacchi remoti.
- **Dialer** - Programmi dannosi progettati per connettersi a numeri con tariffe telefoniche molto elevate anziché ai

provider dei servizi Internet dell'utente. È quasi impossibile che un utente noti che è stata creata una nuova connessione. I dialer possono causare danni solo agli utenti con connessione remota che ormai viene utilizzata sempre meno frequentemente.

Se sul computer in uso viene rilevato un trojan horse, si consiglia di eliminarlo, poiché probabilmente contiene codice dannoso.

6.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono agli autori degli attacchi su Internet l'accesso illimitato a un sistema, nascondendo tuttavia la loro presenza. I rootkit, dopo aver effettuato l'accesso a un sistema (di norma, sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per non essere rilevate dal software antivirus: nascondono i processi, i file e i dati del Registro di sistema di Windows. Per tale motivo, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di testing.

Per bloccare i rootkit, sono disponibili due livelli di rilevamento:

1. Quando tentano di accedere ad un sistema: Non sono ancora presenti e pertanto sono inattivi. La maggior parte dei sistemi antivirus è in grado di eliminare i rootkit a questo livello (presupponendo che riescano effettivamente a rilevare tali file come infetti).
2. Quando sono nascosti dal normale testing: ESET NOD32 Antivirus gli utenti hanno il vantaggio di poter utilizzare la tecnologia Anti-Stealth che è in grado di rilevare ed eliminare anche i rootkit attivi.

6.1.5 Adware

Adware è l'abbreviazione di software con supporto della pubblicità (advertising-supported software). Rientrano in questa categoria i programmi che visualizzano materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenenti pubblicità all'interno di un browser Internet oppure ne modificano la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono ai loro sviluppatori di coprire i costi di sviluppo delle applicazioni che, in genere, sono molto utili.

L'adware non è di per sé pericoloso, anche se gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere anche funzioni di rilevamento e registrazione, al pari dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware.

Alcuni programmi non vengono installati senza adware. In caso contrario, le rispettive funzionalità saranno limitate. Ciò significa che l'adware potrebbe accedere di frequente al sistema in modo "legale", poiché l'utente ne ha dato il consenso. In questi casi, vale il proverbio secondo il quale la prudenza non è mai troppa. Se in un computer viene rilevato un file adware, l'operazione più appropriata è l'eliminazione dello stesso, in quanto esistono elevate probabilità che il file contenga codice dannoso.

6.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso/consapevolezza dell'utente. Gli spyware si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, tra cui un elenco dei siti Web visitati, indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che lo scopo di tali tecniche è raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è legato al fatto che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware sono frequentemente accoppiati a versioni gratuite di un programma creato dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire l'aggiornamento a una versione a pagamento che non lo contiene.

Esempi di prodotti freeware noti associati a programmi spyware sono le applicazioni client delle reti P2P (peer-to-

peer). Spyfalcon o Spy Sheriff (e molti altri ancora) appartengono a una sottocategoria di spyware specifica, poiché si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se in un computer viene rilevato un file spyware, è consigliabile eliminarlo in quanto è molto probabile che contenga codice dannoso.

6.1.7 Programmi di compressione

Un programma di compressione è un eseguibile compresso autoestraente che riunisce vari tipi di malware in un unico pacchetto.

I programmi di compressione più comuni sono UPX, PE_Compact, PKLite e ASPack. Lo stesso malware può essere rilevato in modo diverso se compresso mediante l'utilizzo di un programma di compressione diverso. I programmi di compressione sono anche in grado di mutare le proprie "firme" nel tempo, rendendo più complessi il rilevamento e la rimozione dei malware.

6.1.8 Applicazioni potenzialmente pericolose

Esistono molti programmi legali utili per semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. ESET NOD32 Antivirus offre la possibilità di rilevare tali minacce.

Applicazioni potenzialmente pericolose è la classificazione utilizzata per il software legale e commerciale. Questa classificazione include programmi quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente) rivolgersi all'amministratore di rete o rimuovere l'applicazione.

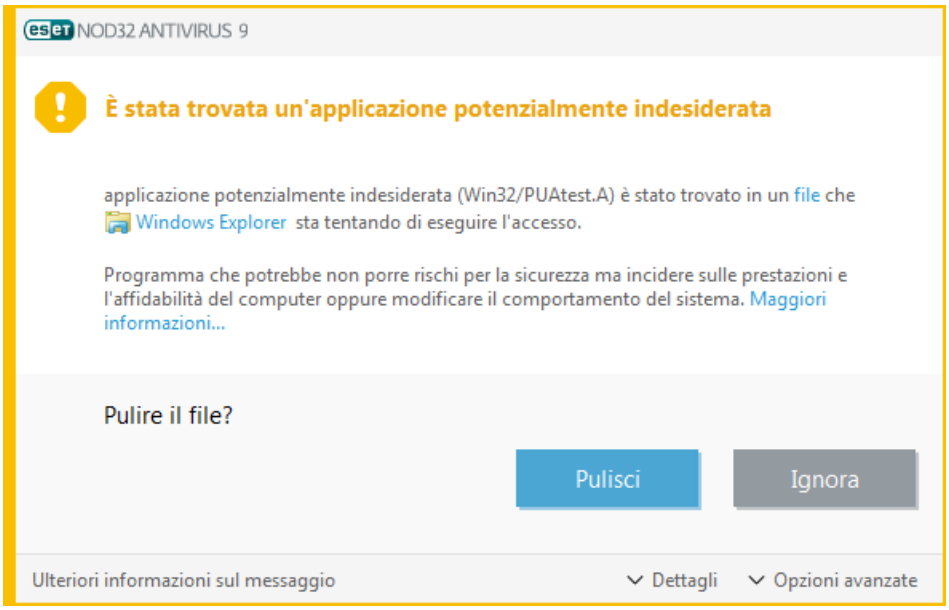
6.1.9 Applicazioni potenzialmente indesiderate

Un'applicazione potenzialmente indesiderata è un programma che contiene adware, installa barre degli strumenti o si prefigge altri obiettivi poco chiari. In alcuni casi, un utente potrebbe percepire che i vantaggi di un'applicazione potenzialmente indesiderata superano i rischi. Per questo motivo, ESET assegna a tali applicazioni una categoria a rischio ridotto rispetto ad altri tipi di software dannosi, come trojan horse o worm.

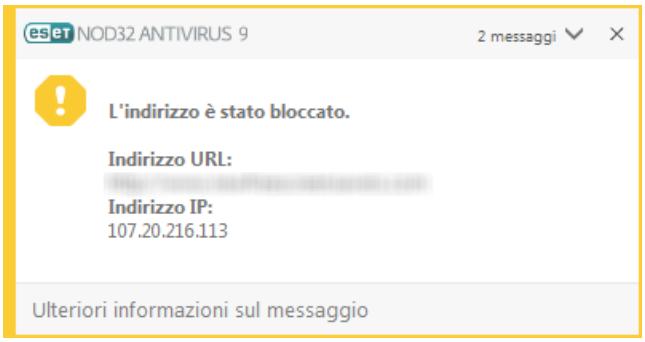
Avviso: trovata minaccia potenziale

In caso di rilevamento di un'applicazione potenzialmente indesiderata, l'utente potrà scegliere l'azione da intraprendere:

1. **Pulisci/Disconnetti**: questa opzione termina l'azione e impedisce alla minaccia potenziale di entrare nel sistema in uso.
2. **Ignora**: questa opzione consente a una minaccia potenziale di entrare nel sistema in uso.
3. Per consentire l'esecuzione futura dell'applicazione sul computer in uso senza interruzioni, fare clic su **Opzioni avanzate** e selezionare la casella di controllo accanto a **Escludi dal rilevamento**.

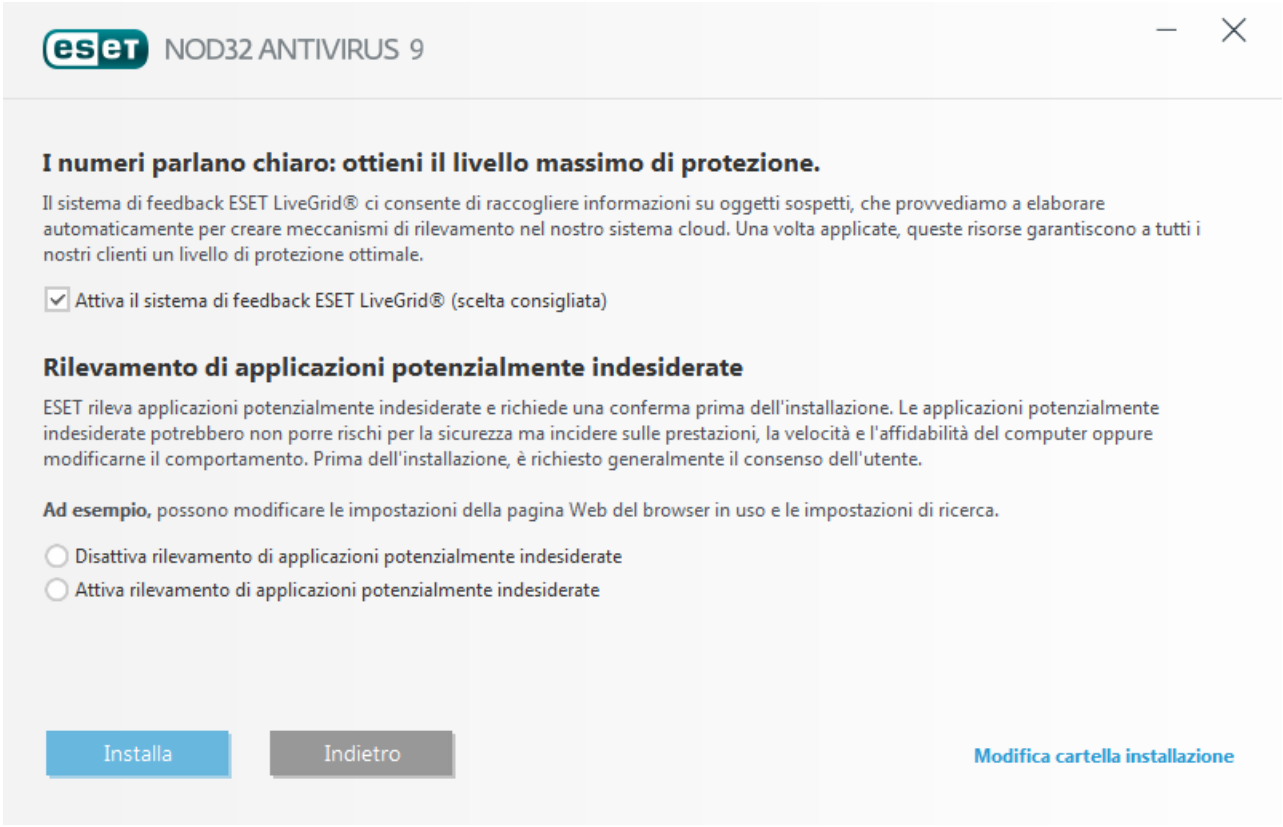

NOD32 ANTIVIRUS 9
È stata trovata un'applicazione potenzialmente indesiderata
applicazione potenzialmente indesiderata (Win32/PUAtest.A) è stato trovato in un file che
Windows Explorer sta tentando di eseguire l'accesso.
Programma che potrebbe non porre rischi per la sicurezza ma incidere sulle prestazioni e l'affidabilità del computer oppure modificare il comportamento del sistema. Maggiori informazioni...
Pulire il file?
Pulisci
Ignora
Ulteriori informazioni sul messaggio
Dettagli
Opzioni avanzate

Se un'applicazione potenzialmente indesiderata viene rilevata e non può essere pulita, verrà visualizzata la finestra di notifica **L'indirizzo è stato bloccato** nell'angolo in basso a destra della schermata. Per ulteriori informazioni su questo evento, accedere a **Strumenti** > **File di rapporto** > **Siti Web filtrati** dal menu principale.



Applicazioni potenzialmente indesiderate: impostazioni

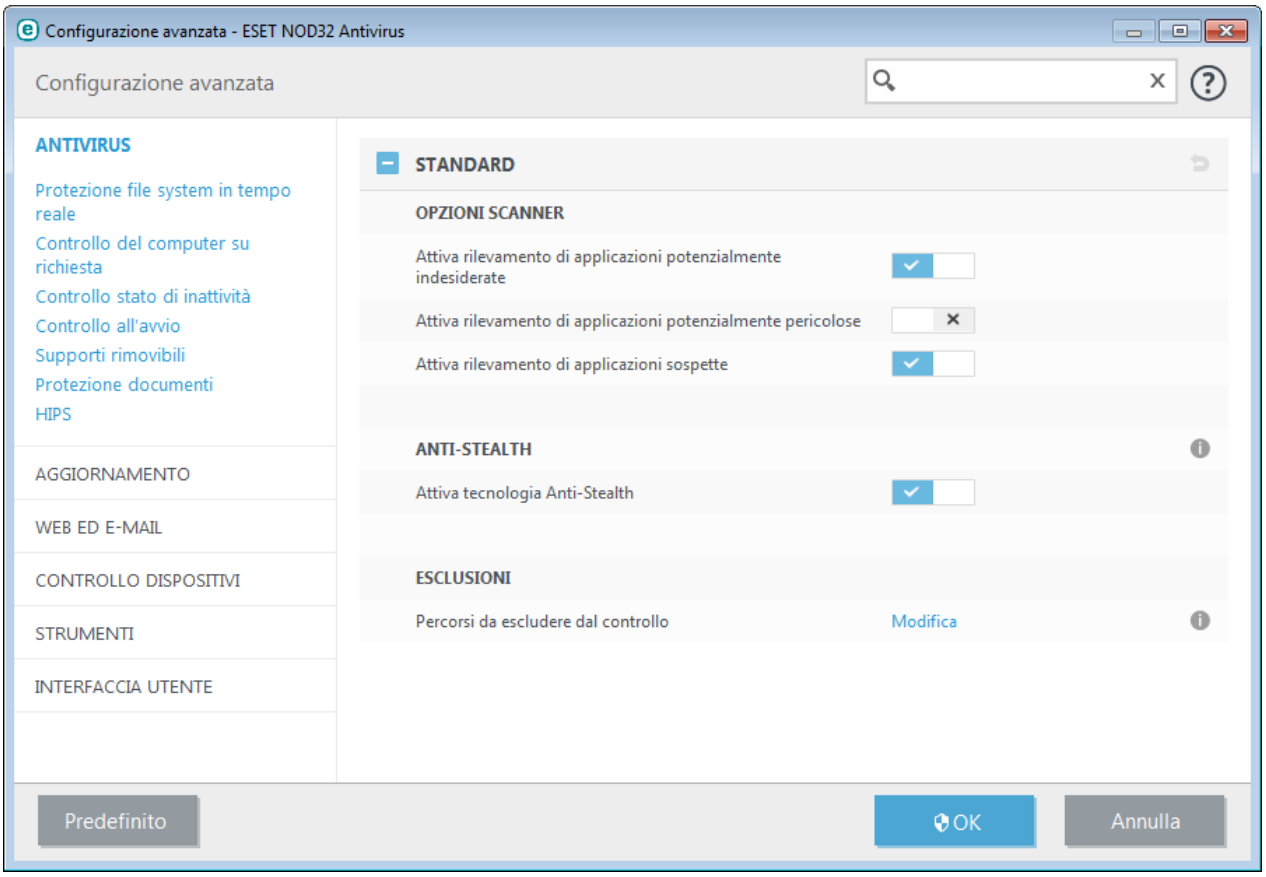
Durante l'installazione di un prodotto ESET, l'utente può decidere di attivare il rilevamento di applicazioni potenzialmente indesiderate, come illustrato di seguito:


NOD32 ANTIVIRUS 9
I numeri parlano chiaro: ottieni il livello massimo di protezione.
Il sistema di feedback ESET LiveGrid® ci consente di raccogliere informazioni su oggetti sospetti, che provvediamo a elaborare automaticamente per creare meccanismi di rilevamento nel nostro sistema cloud. Una volta applicate, queste risorse garantiscono a tutti i nostri clienti un livello di protezione ottimale.
Attiva il sistema di feedback ESET LiveGrid® (scelta consigliata)
Rilevamento di applicazioni potenzialmente indesiderate
ESET rileva applicazioni potenzialmente indesiderate e richiede una conferma prima dell'installazione. Le applicazioni potenzialmente indesiderate potrebbero non porre rischi per la sicurezza ma incidere sulle prestazioni, la velocità e l'affidabilità del computer oppure modificarne il comportamento. Prima dell'installazione, è richiesto generalmente il consenso dell'utente.
Ad esempio, possono modificare le impostazioni della pagina Web del browser in uso e le impostazioni di ricerca.
Disattiva rilevamento di applicazioni potenzialmente indesiderate
Attiva rilevamento di applicazioni potenzialmente indesiderate
Installa
Indietro
Modifica cartella installazione

Le applicazioni potenzialmente indesiderate possono installare adware e barre degli strumenti o contenere altre funzioni di programma non sicure e indesiderate.

Queste impostazioni possono essere modificate in qualsiasi momento. Per attivare o disattivare il rilevamento di applicazioni potenzialmente indesiderate, pericolose o sospette, attenersi alle seguenti istruzioni:

1. Aprire il prodotto ESET. Come faccio ad aprire il mio prodotto ESET?
2. Premere il tasto **F5** per accedere alla **Configurazione avanzata**.
3. Fare clic su **Antivirus** e attivare o disattivare le opzioni **Attiva rilevamento di applicazioni potenzialmente indesiderate**, **Attiva rilevamento di applicazioni potenzialmente pericolose** e **Attiva rilevamento di applicazioni sospette** in base alle proprie preferenze. Confermare facendo clic su **OK**.



Applicazioni potenzialmente indesiderate: wrapper di software

Il wrapper di un software è un tipo speciale di modifica di un'applicazione utilizzato da alcuni siti Web che offrono servizi di file hosting. Si tratta di uno strumento di terze parti che installa il programma che si intende scaricare aggiungendo, però, altri software, come ad esempio barre degli strumenti o adware. I software aggiuntivi possono inoltre apportare modifiche alla pagina iniziale del browser Web in uso e alle impostazioni di ricerca. Inoltre, i siti Web che offrono servizi di file hosting non comunicano al fornitore del software o al destinatario del download le modifiche apportate e non consentono di rifiutarle facilmente. Per tali motivi, ESET classifica i wrapper di software tra le applicazioni potenzialmente indesiderate per consentire agli utenti di decidere se accettare o meno il download.

Per una versione aggiornata di questa pagina della Guida, consultare questo articolo della Knowledge Base ESET.

6.2 Tecnologia ESET

6.2.1 Exploit Blocker

L'Exploit Blocker è progettato per rafforzare i tipi di applicazione comunemente utilizzati come browser Web, lettori PDF, client di posta e componenti di MS Office. Il sistema si basa sul monitoraggio del comportamento dei processi ai fini del rilevamento di attività sospette che potrebbero indicare un exploit.

Nel momento in cui l'Exploit Blocker identifica un processo sospetto, lo interrompe immediatamente e registra i dati relativi alla minaccia, che vengono quindi inviati al sistema cloud di ThreatSense. Le informazioni vengono elaborate dal laboratorio di ricerca ESET e utilizzate ai fini di una maggiore protezione degli utenti contro minacce sconosciute e attacchi zero-day (malware di nuova concezione per i quali non sono disponibili soluzioni preconfigurate).

6.2.2 Scanner memoria avanzato

Lo Scanner memoria avanzato lavora congiuntamente all'Exploit Blocker per rafforzare il livello di protezione contro malware concepiti allo scopo di eludere il rilevamento dei prodotti antimalware mediante l'utilizzo di pratiche di offuscazione e/o crittografia. Qualora i metodi di emulazione o di euristica ordinari non siano in grado di rilevare una minaccia, lo Scanner memoria avanzato identifica il comportamento sospetto ed effettua un controllo delle minacce presenti nella memoria del sistema. Questa soluzione si rivela efficace persino contro i malware che utilizzano pratiche di offuscamento ottimizzate.

Diversamente dall'Exploit Blocker, lo Scanner memoria avanzato rappresenta un metodo post-esecuzione. Ciò implica un rischio di esecuzione di attività dannose prima del rilevamento di una minaccia. Tuttavia, qualora le varie tecniche di rilevamento disponibili non si rivelino efficaci, questo sistema offre un livello aggiuntivo di sicurezza.

6.2.3 ThreatSense

Sviluppato sul sistema avanzato di allarme immediato ThreatSense.Net®, ESET LiveGrid® utilizza i dati inviati dagli utenti ESET di tutto il mondo e li invia al laboratorio di ricerca ESET. Grazie all'invio di campioni e metadati "from the wild" sospetti, ESET LiveGrid® consente a ESET di soddisfare le esigenze dei clienti e di gestire le minacce più recenti in modo tempestivo. I ricercatori dei malware ESET utilizzano le informazioni per creare un'istantanea accurata della natura e dell'ambito delle minacce globali, che consente a ESET di focalizzarsi sugli obiettivi appropriati. I dati ESET LiveGrid® giocano un ruolo importante nella definizione delle priorità nell'ambito dei sistemi di elaborazione automatici.

Questo strumento consente inoltre di implementare un sistema di reputazione che contribuisce al potenziamento dell'efficienza complessiva delle soluzioni anti-malware ESET. Durante l'analisi di un file eseguibile o di un archivio sul sistema di un utente, il relativo hashtag viene dapprima confrontato rispetto a un database di elementi della whitelist e della blacklist. Se presente nella whitelist, il file analizzato viene considerato pulito e contrassegnato ai fini dell'esclusione da controlli futuri. Se presente nella blacklist, verranno intraprese azioni appropriate in base alla natura della minaccia. In caso di mancata corrispondenza, il file viene sottoposto a un controllo completo. Sulla base dei risultati del controllo, i file vengono categorizzati come minacce o non minacce. Questo approccio registra un impatto positivo importante sulle prestazioni del controllo.

Il sistema di reputazione consente di effettuare un rilevamento efficace di campioni di malware anche prima dell'invio delle relative firme al computer dell'utente, mediante il database antivirus aggiornato (tale azione si ripete più di una volta al giorno).

6.2.4 Java Exploit Blocker

Java Exploit Blocker è un'estensione della protezione Exploit Blocker esistente. Monitora Java e ricerca comportamento simile a exploit. I campioni bloccati possono essere segnalati agli analisti di malware i quali possono creare firme per bloccarli su differenti livelli (blocco URL, download di file e così via).

6.3 E-mail

L'e-mail o electronic mail è una moderna forma di comunicazione che presenta numerosi vantaggi. È flessibile, veloce e diretta e ha svolto un ruolo cruciale nella proliferazione di Internet all'inizio degli anni novanta.

Purtroppo, a causa dell'elevato livello di anonimità, i messaggi e-mail e Internet lasciano ampio spazio ad attività illegali come lo spam. Lo spamming include annunci pubblicitari non desiderati, hoax e proliferazione di software dannoso o malware. Ad aumentare ulteriormente i disagi e i pericoli è il fatto che i costi di invio dello spamming sono minimi e gli autori dispongono di numerosi strumenti per acquisire nuovi indirizzi e-mail. Il volume e la varietà dello spamming ne rende inoltre estremamente difficoltoso il monitoraggio. Maggiore è il periodo di utilizzo dell'indirizzo e-mail, più elevata sarà la possibilità che finisca in un database per motori di spamming. Di seguito sono riportati alcuni suggerimenti per la prevenzione di messaggi e-mail indesiderati:

- Se possibile, evitare di pubblicare il proprio indirizzo e-mail su Internet
- Fornire il proprio indirizzo e-mail solo a utenti considerati attendibili
- Se possibile, non utilizzare alias comuni. Maggiore è la complessità degli alias, minore sarà la probabilità che vengano rilevati
- Non rispondere a messaggi di spam già recapitati nella posta in arrivo
- Quando si compilano moduli su Internet, prestare particolare attenzione a selezionare opzioni quali "Sì, desidero ricevere informazioni".
- Utilizzare indirizzi e-mail "specifici", ad esempio uno per l'ufficio, uno per comunicare con gli amici e così via.
- Cambiare di tanto in tanto l'indirizzo e-mail
- Utilizzare una soluzione antispam

6.3.1 Pubblicità

La pubblicità su Internet è una delle forme di pubblicità in maggior crescita. I vantaggi principali dal punto di vista del marketing sono i costi ridotti e un livello elevato di immediatezza. I messaggi vengono inoltre recapitati quasi immediatamente. Molte società utilizzano strumenti di marketing via e-mail per comunicare in modo efficace con i clienti attuali e potenziali.

Questo tipo di pubblicità è legittimo, perché si potrebbe essere interessati a ricevere informazioni commerciali su determinati prodotti. Molte società inviano tuttavia messaggi di contenuto commerciale non desiderati. In questi casi, la pubblicità tramite e-mail supera il limite e diventa spam.

La quantità di messaggi e-mail non desiderati diventa così un problema e non sembra diminuire. Gli autori di messaggi e-mail non desiderati tentano spesso di mascherare i messaggi spam come messaggi legittimi.

6.3.2 Hoax: truffe e bufale

Un hoax è un messaggio contenente informazioni non veritiere diffuso su Internet. che viene in genere inviato via e-mail e tramite strumenti di comunicazione come ICQ e Skype. Il messaggio stesso è in genere una burla o una leggenda metropolitana.

Gli hoax virus tentano di generare paura, incertezza e dubbio (FUD, Fear, Uncertainty and Doubt) nei destinatari, inducendoli a credere che nei relativi sistemi è presente un "virus non rilevabile" in grado di eliminare file e recuperare password o di eseguire altre attività dannose.

Alcuni hoax richiedono ai destinatari di inoltrare messaggi ai loro contatti, aumentandone così la diffusione. Esistono hoax via cellulare, richieste di aiuto, offerte di denaro dall'estero e così via. Spesso è impossibile determinare l'intento dell'autore del messaggio.

È molto prababile che i messaggi che invitano ad essere inoltrati a tutti i propri conoscenti siano hoax. Su Internet sono presenti molti siti Web in grado di verificare l'autenticità di un messaggio e-mail. Prima di inoltrarlo, effettuare una ricerca in Internet per qualsiasi messaggio si sospetti essere hoax.

6.3.3 Phishing

Il termine phishing definisce un'attività illegale che si avvale di tecniche di ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni confidenziali). Lo scopo è quello di ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via.

Di norma, l'accesso viene ricavato tramite l'invio di messaggi e-mail che imitano quelli di una persona o società affidabile (istituto finanziario, compagnia di assicurazioni). Il messaggio e-mail sembra autentico e presenta immagini e contenuti che possono indurre a credere che provenga effettivamente da un mittente affidabile. Tali messaggi chiedono all'utente, con vari pretesti (verifica dati, operazioni finanziarie), di immettere alcuni dati personali: numeri di conto bancario o nomi utente e password. Tali dati, se inviati, possono essere rubati e utilizzati in modo illegale.

Le banche, le compagnie di assicurazioni e altre società legittime non chiederanno mai di rivelare nomi utente e password in messaggi e-mail non desiderati.

6.3.4 Riconoscimento messaggi spamming

In genere, esistono alcuni indicatori che consentono di identificare i messaggi spamming (e-mail non desiderate) nella cassetta postale. Un messaggio può essere considerato un messaggio spamming se soddisfa almeno alcuni dei criteri riportati di seguito.

- L'indirizzo del mittente non appartiene a nessuno degli utenti presenti nell'elenco dei contatti.
- Agli utenti viene offerta una grossa somma di denaro, purché si impegnino tuttavia ad anticipare una piccola somma di denaro.
- Viene chiesto di immettere con vari pretesti (verifica di dati, operazioni finanziarie) alcuni dati personali, quali numero di conto bancario, nome utente, password e così via.
- È scritto in una lingua straniera.
- Viene chiesto di acquistare un prodotto a cui non si è interessati. Se tuttavia si decide di acquistarlo, è consigliabile verificare che il mittente del messaggio sia un fornitore attendibile (contattare il produttore originale).
- Alcuni termini contengono errori di ortografia nel tentativo di aggirare il filtro di spamming, ad esempio "vaigra" invece di "viagra" e così via

7. Domande comuni

In questo capitolo sono illustrate alcune delle domande frequenti e i problemi riscontrati. Fare clic sul titolo dell'argomento per trovare la soluzione al problema:

Come aggiornare ESET NOD32 Antivirus
Come rimuovere un virus dal PC
Come creare una nuova attività nella Pianificazione attività
Come pianificare un'attività di scansione (ogni 24 ore)

Se non è stato possibile trovare la soluzione del problema nelle pagine della Guida di cui sopra, consultare le pagine della guida di ESET NOD32 Antivirus.

Se non è stato possibile trovare la soluzione a un problema o la risposta a una domanda nelle pagine della Guida, consultare la Knowledge Base ESET on-line, sottoposta a periodici aggiornamenti. Seguono i collegamenti ai principali articoli della Knowledge base per la risoluzione di problemi comuni:

Durante l'installazione del prodotto ESET visualizzo un messaggio di errore. Cosa significa?
Come faccio a inserire il Nome utente e la Password in ESET Smart Security/ESET NOD32 Antivirus?
Ho ricevuto un messaggio relativo al termine anticipato della mia installazione ESET
Cosa devo fare dopo aver rinnovato la licenza? (utenti Home)
Cosa succede se modifico il mio indirizzo di posta elettronica?
Come faccio ad avviare Windows in Modalità provvisoria o in Modalità provvisoria senza rete?

Se necessario, contattare il Supporto tecnico per eventuali domande o problemi riscontrati. Il modulo di contatto è disponibile nella scheda **Guida e supporto tecnico** di ESET NOD32 Antivirus.

7.1 Come aggiornare ESET NOD32 Antivirus

L'aggiornamento di ESET NOD32 Antivirus può essere eseguito manualmente o automaticamente. Per avviare l'aggiornamento, fare clic su **Aggiorna adesso** nella sezione **Aggiorna**.

Le impostazioni predefiniti dell'installazione consentono di creare un'attività di aggiornamento automatica che viene eseguita ogni ora. Se occorre modificare l'intervallo, accedere a **Strumenti** > **Pianificazione attività** (per ulteriori informazioni sulla Pianificazione attività, fare clic qui).

7.2 Come rimuovere un virus dal PC

Se il computer mostra sintomi di infezione malware, ad esempio appare più lento o si blocca spesso, è consigliabile attenersi alle seguenti istruzioni:

1. Nella finestra principale del programma, fare clic su **Controllo computer**.
2. Fare clic su **Controllo computer** per avviare il controllo del sistema.
3. Al termine del controllo, verificare nel registro il numero di file sottoposti a controllo, file infetti e file puliti.
4. Se si desidera controllare solo una parte del disco, fare clic su **Controllo personalizzato** e selezionare gli oggetti da controllare per la ricerca di virus.

Per ulteriori informazioni, consultare l'articolo della Knowledge Base ESET aggiornato periodicamente.

7.3 Come creare una nuova attività nella Pianificazione attività

Per creare una nuova attività in **Strumenti** > **Pianificazione attività**, fare clic su **Aggiungi** oppure fare clic con il pulsante destro del mouse e selezionare **Aggiungi...** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione esterna** - Consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto** - File di rapporto contenenti elementi rimasti dai record eliminati. Questa attività ottimizza periodicamente i record nei file di rapporto allo scopo di garantire un funzionamento efficiente.
- **Controllo del file di avvio del sistema** - Consente di controllare i file la cui esecuzione è consentita all'avvio del sistema o all'accesso.
- **Crea snapshot di stato computer** - Crea uno snapshot del computer ESET SysInspector - raccoglie informazioni dettagliate sui componenti del sistema (ad esempio, driver e applicazioni) e valuta il livello di rischio di ciascun componente.
- **Controllo computer su richiesta** - Consente di eseguire un controllo di file e di cartelle sul computer in uso.
- **Primo controllo** - Per impostazione predefinita, 20 minuti dopo l'installazione o il riavvio, verrà eseguito un Controllo del computer come attività con priorità bassa.
- **Aggiorna**: pianifica un'attività di aggiornamento aggiornando il database delle firme antivirali e i moduli del programma.

Poiché **Aggiorna** rappresenta una delle attività pianificate utilizzata con maggiore frequenza, di seguito verranno illustrate le modalità in cui è possibile aggiungere una nuova attività di aggiornamento:

Dal menu a discesa **Attività pianificata**, selezionare **Aggiorna**. Inserire il nome dell'attività nel campo **Nome attività** e fare clic su **Avanti**. Selezionare la frequenza dell'attività. Sono disponibili le seguenti opzioni: **Una volta**, **Ripetutamente**, **Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento.** Selezionare **Ignora attività se in esecuzione su un computer alimentato dalla batteria** per ridurre al minimo le risorse di sistema in caso di utilizzo della batteria del computer portatile. L'attività verrà eseguita alla data e all'ora specificate nei campi **Esecuzione attività**. È quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le seguenti opzioni:

- **Al prossimo orario pianificato**
- **Prima possibile**
- **Immediatamente, se l'ora dall'ultima esecuzione supera un valore specificato** (è possibile definire l'intervallo utilizzando la casella di scorrimento **Ora dall'ultima esecuzione (ore)**)

Nel passaggio successivo, viene visualizzata una finestra contenente un riepilogo delle informazioni sull'attività pianificata corrente. Fare clic su **Fine** una volta terminate le modifiche.

Verrà visualizzata una finestra di dialogo in cui è possibile scegliere i profili da utilizzare per l'attività pianificata. Qui è possibile impostare il profilo primario e alternativo. Il profilo alternativo viene utilizzato se l'attività non può essere completata mediante l'utilizzo del profilo primario. Confermare facendo clic su **Fine**. A questo punto, la nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

7.4 Come pianificare un controllo del computer settimanale

Per programmare un'attività periodica, aprire la finestra principale del programma e fare clic su **Strumenti** > **Pianificazione attività**. Di seguito viene riportata la procedura da seguire per pianificare un'attività che controllerà tutti i dischi locali ogni 24 ore. Per ulteriori istruzioni dettagliate, consultare l'articolo della Knowledge Base ESET.

Per pianificare un'attività di scansione:

1. Fare clic su **Aggiungi** nella schermata principale di Pianificazione attività.
2. Selezionare **Controllo computer su richiesta** dal menu a discesa.
3. Immettere un nome per l'attività, quindi selezionare **Ogni settimana** per impostare la frequenza dell'attività.
4. Impostare l'ora e il giorno di esecuzione dell'attività.

5. Selezionare **Esegui l'attività appena possibile** per eseguire l'attività in un secondo momento nel caso in cui, per qualsiasi motivo, l'esecuzione dell'attività pianificata non si avvia (ad esempio se il computer era spento).
6. Esaminare il riepilogo dell'attività pianificata e fare clic su **Fine**.
7. Selezionare **Unità locali** nel menu a discesa **Destinazioni**.
8. Fare clic su **Fine** per confermare l'attività.